REGULATOR CONSTANTS AND THE PARITY CONJECTURE

TIM† AND VLADIMIR DOKCHITSER

Abstract. The p-parity conjecture for twists of elliptic curves relates multiplicities of Artin representations in p^∞-Selmer groups to root numbers. In this paper we prove this conjecture for a class of such twists. For example, if $E/\mathbb{Q}$ is semistable at 2 and 3, $K/\mathbb{Q}$ is abelian and K^∞ is its maximal pro-p extension, then the p-parity conjecture holds for twists of E by all orthogonal Artin representations of $\mathrm{Gal}(K^\infty/\mathbb{Q})$. We also give analogous results when $K/\mathbb{Q}$ is non-abelian, the base field is not $\mathbb{Q}$ and E is replaced by an abelian variety. The heart of the paper is a study of relations between permutation representations of finite groups, their "regulator constants", and compatibility between local root numbers and local Tamagawa numbers of abelian varieties in such relations.

Contents

Date: March 21, 2009.
MSC 2000: Primary 11G05; Secondary 11G07, 11G10, 11G40, 19A22, 20B99.
†Supported by a Royal Society University Research Fellowship.

1. Introduction

The emphasis of this paper is twofold: to study the interplay between functions on G-sets and on G-representations for a finite group G, and to use it to link root numbers and Tamagawa numbers of abelian varieties. The main application is the parity conjecture for classes of twists of elliptic curves and abelian varieties by Artin representations.

1.i. **Parity conjectures.** Consider an abelian variety A defined over a number field K, and a Galois extension F/K. The Galois group $\mathrm{Gal}(F/K)$ acts on the F-rational points of A, and an extension of the Birch–Swinnerton-Dyer conjecture relates the multiplicities of complex representations in $A(F)\otimes\mathbb{C}$ to the order of vanishing of the corresponding twisted L-functions at $s=1$:

Conjecture 1.1 (Birch–Swinnerton-Dyer–Deligne–Gross; [40, 4], [28] §2)**.** *For every complex representation τ of $\mathrm{Gal}(F/K)$,*

$$\langle\tau, A(F)\rangle = \mathrm{ord}_{s=1} L(A,\tau,s).$$

(Here and below $\langle\tau,*\rangle$ is the usual representation-theoretic inner product of τ and the complexification of $*$.) When τ is self-dual, the parity of the right-hand side is forced by the sign in the conjectural functional equation, the global root number $w(A/K,\tau)$. Thus, we expect

$$(-1)^{\langle\tau,A(F)\rangle} = w(A/K,\tau).$$

There is an analogous picture for Selmer groups. For a prime p, let

$$\mathcal{X}_p(A/K) = \big(\text{Pontryagin dual of the } p^\infty\text{-Selmer group of } A/K\big) \otimes \mathbb{Q}_p.$$

This is a $\mathbb{Q}_p$-vector space whose dimension is simply the Mordell-Weil rank of A/K plus the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ in the Tate-Shafarevich group Ш(A/K). The conjectural finiteness of Ш then suggests the following parity statements, which are often much more accessible:

Conjecture 1.2a (p-Parity Conjecture)**.**

$$(-1)^{\dim \mathcal{X}_p(A/K)} = w(A/K).$$

Similarly, for a self-dual representation τ of $\mathrm{Gal}(F/K)$, we expect

Conjecture 1.2b (p-Parity Conjecture for twists)**.**

$$(-1)^{\langle\tau,\mathcal{X}_p(A/F)\rangle} = w(A/K,\tau).$$

When $K\subset L\subset F$, the second statement for the permutation representation on the set of K-embeddings $L\hookrightarrow F$ is equivalent to the first one for A/L. So 1.2b for all orthogonal twists implies 1.2a over all intermediate fields of F/K.

The main applications of this paper confirm special cases of Conjecture 1.2b. Here are two specific examples:

Theorem 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve, semistable at 2 and 3. Suppose $F/\mathbb{Q}$ is Galois and the commutator subgroup of $G=\mathrm{Gal}(F/\mathbb{Q})$ is a p-group. Then the p-parity conjecture holds for twists of E by all orthogonal representations of G and, in particular, over all subfields of F.*

Theorem 1.4. *Let p be an odd prime, and suppose F/K is Galois and $P \lhd \mathrm{Gal}(F/K)$ is a p-subgroup. Let A/K be a principally polarised abelian variety whose primes of unstable reduction are unramified in F/K. If the p-parity conjecture holds for A over the subfields of F^P/K, then it holds over all subfields of F/K.*

The general results on the p-parity conjecture (Theorems 1.6, 1.11 and 1.12) are given in §1.iii. But first we introduce our main tool from group theory, which may be of independent interest.

1.ii. **G-sets versus G-representations.** Let G be an abstract finite group. Suppose $\phi : H \mapsto \phi(H)$ is a function that associates to every subgroup $H < G$ a value in some abelian group $\mathcal{A}$ (written multiplicatively), and that ϕ takes the same value on conjugate subgroups. Recall that $H \leftrightarrow G/H$ is a bijection between subgroups of G up to conjugacy and transitive G-sets up to isomorphism. So ϕ extends to a map from all G-sets to $\mathcal{A}$ by the rule $\phi(X \amalg Y) = \phi(X)\phi(Y)$. Let us call ϕ "representation-theoretic" if $\phi(X)$ only depends on the representation $\mathbb{C}[X]$.

Alternatively, say that a formal combination of (conjugacy classes of) subgroups $\Theta = \sum_i n_i H_i$ is a *relation between permutation representations of* G, or simply a *G-relation*, if

$$\bigoplus_i \mathbb{C}[G/H_i]^{\oplus n_i} \cong 0,$$

as a virtual representation, i.e. the character $\sum_i n_i \chi_{\mathbb{C}[G/H_i]}$ is zero. Then for ϕ to be representation-theoretic is equivalent to $\prod_i \phi(H_i)^{n_i}$ being 1 for every such G-relation.

For example, $G = \mathrm{S}_3$ has a unique relation up to multiples,

$$\Theta = 2\mathrm{S}_3 + \{1\} - 2\mathrm{C}_2 - \mathrm{C}_3 \,.$$

(i.e. $\mathbf{1}^{\oplus 2} \oplus \mathbb{C}[\mathrm{S}_3] \cong \mathbb{C}[\mathrm{S}_3/\mathrm{C}_2]^{\oplus 2} \oplus \mathbb{C}[\mathrm{S}_3/\mathrm{C}_3]$; clearly such a relation must exist: S_3 has 4 subgroups up to conjugacy, but only 3 irreducible representations.)

In the context of number theory, G may be a Galois group of a number field $F/\mathbb{Q}$, and $\phi(H)$ some invariant of the intermediate field F^H. For instance, $\phi(H)$ could be the the degree of F^H, its discriminant, class number or Dedekind zeta-function $\zeta_{F^H}(s)$ (with $\mathcal{A} = \mathbb{Z}, \mathbb{Q}^\times, \mathbb{Q}^\times$ and the group of non-zero meromorphic functions on $\mathbb{C}$, respectively). Of these four, all but the class number are representation-theoretic, e.g. $[F^H : \mathbb{Q}] = \dim \mathbb{C}[G/H]$ and $\zeta_{F^H}(s) = L(\mathbb{C}[G/H], s)$ are visibly functions of $\mathbb{C}[G/H]$. It follows, for example, that in every S_3-extension $F/\mathbb{Q}$,

$$\zeta(s)^2 \zeta_F(s) = \zeta_{F^{\mathrm{C}_2}}(s)^2 \zeta_{F^{\mathrm{C}_3}}(s).$$

The class number formula then yields an explicit identity between the corresponding class numbers and regulators ($\frac{h \cdot \mathrm{Reg}}{|\mu|}$ is representation-theoretic).

We are going to study extensively G-relations and functions on G-relations, and present techniques for verifying when a function or a quotient of two such functions is representation-theoretic (see §2).

Regulator constants. Of particular interest to us is the function

$$\mathfrak{D}_\rho : H \mapsto \det(\tfrac{1}{|H|}\langle,\rangle|\rho^H) \in \mathcal{K}^\times/\mathcal{K}^{\times 2}$$

that, for a fixed self-dual $\mathcal{K}G$-representation ρ ($\mathcal{K}$ a field) with a G-invariant pairing $\langle,\rangle$, computes the determinant of the matrix representing $\frac{1}{|H|}\langle,\rangle$ on any basis of the H-invariants ρ^H. Its significance will become clear when we discuss functions coming from abelian varieties. The fundamental property of $\mathfrak{D}_\rho$ is that if $\langle\!\langle,\rangle\!\rangle$ is another pairing on ρ, then $\mathfrak{D}_\rho^{\langle,\rangle}/\mathfrak{D}_\rho^{\langle\!\langle,\rangle\!\rangle}$ is representation-theoretic. In other words, for every G-relation $\Theta = \sum_i n_i H_i$, the quantity

$$\mathcal{C}_\Theta(\rho) = \prod_i \mathfrak{D}_\rho(H_i)^{n_i} \in \mathcal{K}^\times/\mathcal{K}^{\times 2}$$

is independent of the pairing. Following [6] we call $\mathcal{C}_\Theta(\rho)$ the *regulator constant* of ρ. (Their properties are discussed in §2.ii and §2.iv.)

Example 1.5. Suppose $G = \mathrm{D}_{2p^n}$ is dihedral with $p \neq 2$, and $\mathcal{K} = \mathbb{Q}$ or $\mathbb{Q}_p$. The smallest subgroups $\{1\}, \mathrm{C}_2, \mathrm{C}_p$ and D_{2p} form a G-relation

$$\Theta = \{1\} + 2\,\mathrm{D}_{2p} - \mathrm{C}_p - 2\,\mathrm{C}_2\ .$$

The irreducible $\mathcal{K}G$-representations are $\mathbf{1}$ (trivial), ϵ (sign) and ρ_k of dimension $p^k - p^{k-1}$ for every $1 \le k \le n$; they are all self-dual. An elementary computation (see Examples 2.20, 2.21) shows that

$$\mathcal{C}_\Theta(\mathbf{1}) = \mathcal{C}_\Theta(\epsilon) = \mathcal{C}_\Theta(\rho_n) = p, \qquad \mathcal{C}_\Theta(\rho_k) = 1 \quad (1 \le k < n).$$

1.iii. **Main results and applications.** The central result of this paper is the p-parity conjecture for the following twists: for a group G, a prime p and a G-relation Θ, define $\mathbf{T}_{\Theta,p}$ to be the set of self-dual $\bar{\mathbb{Q}}_pG$-representations τ that satisfy

$$\langle \tau, \rho \rangle \equiv \operatorname{ord}_p \mathcal{C}_\Theta(\rho) \mod 2$$

for every self-dual $\mathbb{Q}_pG$-representation ρ (computing $\mathcal{C}_\Theta(\rho)$ with $\mathcal{K} = \mathbb{Q}_p$).

Theorem 1.6(a). *Let F/K be a Galois extension of number fields. Suppose E/K is an elliptic curve whose primes of additive reduction above 2 and 3 have cyclic decomposition groups (e.g. are unramified) in F/K. For every p and every relation Θ between permutation representations of* $\mathrm{Gal}(F/K)$*,*

$$(-1)^{\langle \tau, \mathcal{X}_p(E/F)\rangle} = w(E/K,\tau) \qquad \textit{for all } \tau \in \mathbf{T}_{\Theta,p}.$$

Theorem 1.6(b). *Let F/K be a Galois extension of number fields. Suppose A/K is a principally polarised abelian variety whose primes of unstable reduction have cyclic decomposition groups in F/K. Let p be a prime, and assume that either*

- *$p \neq 2$, or*
- *$p = 2$, the principal polarisation is induced by a K-rational divisor, and A has split semistable reduction at primes $v|2$ of K which have non-cyclic wild inertia group in F/K.*

For every relation Θ between permutation representations of $\mathrm{Gal}(F/K)$*,*

$$(-1)^{\langle \tau, \mathcal{X}_p(A/F)\rangle} = w(A/K,\tau) \qquad \textit{for all } \tau \in \mathbf{T}_{\Theta,p}.$$

Remark 1.7. In particular, if p is odd, Conjecture 1.2b holds for $\tau \in \mathbf{T}_{\Theta,p}$ for all semistable principally polarised abelian varieties over K.

Remark 1.8. In general, the representations in $\mathbf{T}_{\Theta,p}$ simply encode the regulator constants. For instance, if $\{\rho_j\}$ are the irreducible self-dual $\mathbb{Q}_pG$-representations with $\operatorname{ord}_p \mathcal{C}_\Theta(\rho_j)$ odd, then

$$\bigoplus_j (\text{any } \bar{\mathbb{Q}}_p\text{-irreducible constituent of } \rho_j) \ \in\ \mathbf{T}_{\Theta,p}\,.$$

(This representation is automatically self-dual by Corollary 2.25). A general element in $\mathbf{T}_{\Theta,p}$ differs from this one by an element of $\mathbf{T}_{0,p}$, a representation for which the p-parity conjecture ought to "trivially" hold; it would be very interesting to have an intrinsic description of $\bigcup_\Theta \mathbf{T}_{\Theta,p}$, cf. Remarks 2.51, 2.58.

Example 1.9 ($\operatorname{Gal}(F/K) = \mathrm{D}_{2p^n}$, p odd)**.** Continuing Example 1.5, for every $\bar{\mathbb{Q}}_p$-irreducible (2-dimensional) constituent τ_n of ρ_n,

$$\mathbf{1} \oplus \epsilon \oplus \tau_n \ \in\ \mathbf{T}_{\Theta,p}\,.$$

If A/K is an abelian variety that satisfies the assumptions of Theorem 1.6, e.g. A is semistable at primes that ramify in F/K, the p-parity conjecture holds for the twist of A by $\mathbf{1} \oplus \epsilon \oplus \tau_n$. Applying this construction to the D_{2p^k}-quotients of D_{2p^n}, we deduce the p-parity conjecture for the twists of A by $\mathbf{1}\oplus\epsilon\oplus\tau$ for every 2-dimensional irreducible representation τ of $\operatorname{Gal}(F/K)$.

As the p-parity conjecture is known to hold for elliptic curves over $\mathbb{Q}$, and therefore for their quadratic twists as well, we find

Corollary 1.10 (Parity conjecture in anticyclotomic towers)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, L an imaginary quadratic field and p an odd prime. If $p=3$, assume that either E is semistable at 3 or that 3 splits in L. Then for every layer L_n of the $\mathbb{Z}_p$-anticyclotomic extension of L and every representation τ of* $\operatorname{Gal}(L_n/\mathbb{Q})$,

$$\operatorname{ord}_{s=1} L(E,\tau,s) \equiv \langle \tau, \mathcal{X}_p(E/L_n)\rangle \mod 2.$$

In §4 we generalise Example 1.9 to other groups with a large normal p-subgroup. Based on Theorem 1.6, and using purely group-theoretic manipulations we obtain (see Theorems 4.5, 4.2)

Theorem 1.11. *Suppose F/K is a Galois extension of number fields and the commutator subgroup of $G = \operatorname{Gal}(F/K)$ is a p-group. Let A/K be an abelian variety satisfying the hypotheses of Theorem 1.6. If the p-parity conjecture holds for A over K and its quadratic extensions in F, then it holds for all twists of A by orthogonal representations of G.*

When $A=E$ is an elliptic curve and $K=\mathbb{Q}$, the assumption on the p-parity conjecture is always satisfied, as we remarked above (in particular, we get Theorem 1.3). It also holds for those E/K that admit a rational p-isogeny under mild restrictions on E at primes above p; see Remark 4.6 for precise statements, an extension to abelian varieties and a list of references.

The condition that the commutator of G is a p-group is equivalent to the Sylow p-subgroup being normal with an abelian quotient. In other words, F should be a p-extension of an abelian extension of the ground field. For instance, the theorem applies when

- G is abelian (any p).
- $G \cong \mathrm{D}_{2p^n}$ is dihedral.
- G is a 2-group and $p = 2$.
- G is an extension of C_2 by a p-group.
- $G \cong (\mathbb{Z}/p^n\mathbb{Z}) \rtimes (\mathbb{Z}/p^n\mathbb{Z})^\times$, for instance $F = \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{m})$, $K = \mathbb{Q}$.
- $G \subset \left(\begin{smallmatrix} * & * \\ p* & * \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, for instance $F = K(C[p^n])$ for some elliptic curve C/K that admits a rational p-isogeny.

Root numbers and parities of Selmer ranks in the last 3 cases have recently been studied by Mazur–Rubin [20, 21], Hachimori–Venjakob [15] and one of us (V.) [8], Rohrlich [31] and Coates–Fukaya–Kato–Sujatha [3]; see also Greenberg's preprint [12]. This kind of extensions arise in non-commutative Iwasawa theory, where one has a tower $F_\infty = \bigcup F_n$ with $\mathrm{Gal}(F_\infty/K)$ a p-adic Lie group. The $\mathrm{Gal}(F_n/K)$ all have a "large" normal p-subgroup with a fixed "small" quotient. When this quotient is *non-abelian*, we have a weaker version of Theorem 1.11 (Theorems 4.3, 4.2; cf. also 4.4 for $p = 2$):

Theorem 1.12. *Suppose F/K is Galois and $P \triangleleft \mathrm{Gal}(F/K)$ is a p-subgroup with $p \neq 2$. Let E/K be an elliptic curve (resp. principally polarised abelian variety) whose primes of additive reduction above 2, 3 (resp. all primes of unstable reduction) have cyclic decomposition groups in F/K. If the p-parity conjecture holds for E over the subfields of F^P/K, then it holds over all subfields of F/K.*

Example 1.13. Let $E/\mathbb{Q}$ be an elliptic curve, semistable at 2 and 3. Take $p \neq 2$ and $F_n = \mathbb{Q}(E[p^n])$, so $\mathrm{Gal}(F_n/\mathbb{Q}) < \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. If the p-parity conjecture holds over the subfields of the first layer $\mathbb{Q}(E[p])/\mathbb{Q}$, then it holds over all subfields of F_n for all n. Incidentally, for $p = 3$ the "first layer" assumption is always satisfied (see Example 4.8).

Using the above theorems, it is also possible to get a lower estimate on the growth of the p^∞-Selmer group in this tower by computing root numbers. For example, if $p \equiv 3 \mod 4$ and E is semistable and admits a rational p-isogeny, then combining Theorem 1.3 and [31] Cor. 2 shows that $\dim \mathcal{X}_p(E/F_n) \geq ap^{2n}$ for some $a > 0$ and large enough n.

Finally, let us point out some of the things that definitely can *not* be obtained just from Theorem 1.6. It is tempting to try and prove the p-parity conjecture for A/K itself by finding a clever extension F/K and a $\mathrm{Gal}(F/K)$-relation Θ with $\mathbf{1} \in \mathbf{T}_{\Theta,p}$. However, Theorem 2.56 shows that all $\tau \in \mathbf{T}_{\Theta,p}$ are even-dimensional (and have trivial determinant). So, even assuming finiteness of Ш and using several primes p, one requires at least one additional twist for which parity is known. For instance, the p-parity conjecture for all elliptic curves over $\mathbb{Q}$ can be proved for odd p by reversing the argument in 1.9 and 1.10: it is possible to find a suitable anticyclotomic extension

where one knows p-parity for the twists by ϵ and some 2-dimensional irreducible τ, whence it is also true for $\mathbf{1}$. (This is the argument used in [6].)

It is also worth mentioning that if ρ is an irreducible $\mathbb{Q}_pG$-representation which is either symplectic or of the form $\sigma\oplus\sigma^*$ over $\bar{\mathbb{Q}}_p$, then $(-1)^{\langle\tau,\rho\rangle}=1$ for every Θ and $\tau\in\mathbf{T}_{\Theta,p}$, so Theorem 1.6 yields no information about the parity of such ρ in $\mathcal{X}_p(A/F)$. Also, the theorem gives no interesting p-parity statements when $p\nmid|G|$ or G has odd order.

For a summary of properties of $\tau\in\mathbf{T}_{\Theta,p}$ and examples see §2.iv.

1.iv. **Regulator constants and parity of Selmer ranks.** To explain our approach to the parity conjecture, let us first review the method of [6, 7] which allows one to express the Selmer parity in Theorem 1.6 in terms of local invariants of the abelian variety.

Suppose F/K is a Galois extension of number fields. For simplicity, consider an elliptic curve E/K, and assume for the moment that the Tate-Shafarevich group Ш is finite. Define the *Birch–Swinnerton-Dyer quotient*

$$\mathrm{BSD}(E/K)=\frac{\mathrm{Reg}_{E/K}\ |\text{Ш}(E/K)|}{\sqrt{|\Delta_K|}\ |E(K)_{\mathrm{tors}}|^2}\cdot C_{E/K},$$

the conjectural leading term of $L(E/K,s)$ at $s\!=\!1$, see [40] §1. Here Reg is the regulator, $C_{E/K}=\prod_v C_v(E/K_v,\omega)$ the product of local Tamagawa numbers and periods, and Δ_K is the discriminant of K (see §1.vi for the notation).

Whenever E_i/K_i are elliptic curves (or abelian varieties) that happen to satisfy $\prod_i L(E_i/K_i,s)^{n_i}=1$, then $\prod_i \mathrm{BSD}(E_i/K_i)^{n_i}=1$ as predicted by the Birch–Swinnerton-Dyer conjecture[1]. Taking the latter modulo rational squares (to eliminate Ш and torsion) yields a relation between the regulators and the local terms C. It turns out, and has already been exploited in [5, 6], that this has strong implications for parities of ranks.

As a first example, if E admits a K-rational *p-isogeny* $E\to E'$, then the equality $L(E/K,s)=L(E'/K,s)$ leads to the congruence

$$\frac{C_{E/K}}{C_{E'/K}}\equiv\frac{\mathrm{Reg}_{E'/K}}{\mathrm{Reg}_{E/K}}\equiv p^{\mathrm{rk}(E/K)}\mod \mathbb{Q}^{\times 2},$$

where the second step is an elementary computation with height pairings.

As a second example, if E/K is arbitrary and E_d/K is its *quadratic twist* by $d\in K^\times$, then $L(E/K,s)L(E_d/K,s)=L(E/K(\sqrt{d}),s)$, and

$$\left|\frac{\Delta^{1/2}_{K(\sqrt{d})}}{\Delta_K}\right|\frac{C_{E/K}C_{E_d/K}}{C_{E/K(\sqrt{d})}}\equiv\frac{\mathrm{Reg}_{E/K(\sqrt{d})}}{\mathrm{Reg}_{E/K}\,\mathrm{Reg}_{E_d/K}}\equiv 2^{\mathrm{rk}(E/K(\sqrt{d}))}\mod\mathbb{Q}^{\times 2}.$$

[1]If $\prod L(E_i/F_i,s)=\prod L(E'_j/F'_j,s)$, the corresponding products of Weil restrictions to $\mathbb{Q}$ have the same L-function, hence isomorphic l-adic representations (Serre [35] §2.5 Rmk. (3)), and are therefore isogenous (Faltings [9]). This is sufficient, as Ш is assumed finite and BSD-quotients are invariant under Weil restriction (Milne [22] §1) and isogeny (Tate–Milne [23] Thm. 7.3).

The main subject of this paper is another massive source of identities between L-functions, *relations between permutation representations.* If F/K is a Galois extension with Galois group G, then a G-relation

$$\Theta: \ \bigoplus_i \mathbb{C}[G/H_i]^{\oplus n_i} = 0 \qquad (H_i < G,\ n_i \in \mathbb{Z})$$

forces the identity $\prod L(E/F^{H_i}, s)^{n_i} = 1$ by Artin formalism, which leads to $\prod (C_{E/F^{H_i}})^{-n_i} \equiv \prod (\mathrm{Reg}_{E/F^{H_i}})^{n_i} \mod \mathbb{Q}^{\times 2}$. By definition of the regulator,

$$\mathrm{Reg}_{E/F^{H_i}} = \det(\tfrac{1}{|H_i|}\langle,\rangle|\rho^{H_i}) \qquad (= \mathfrak{D}_\rho(H_i) \text{ of §1.ii})$$

where $\rho = E(F)\otimes\mathbb{Q}$ and $\langle,\rangle$ is the height pairing on E/F. So the multiplicities $\mathrm{rk}_\sigma(E/F)$ with which various irreducible $\mathbb{Q}G$-representations σ occur in $E(F)\otimes\mathbb{Q}$ satisfy

$$\prod_i (C_{E/F^{H_i}})^{-n_i} \equiv \prod_i (\mathrm{Reg}_{E/F^{H_i}})^{n_i} \equiv \mathcal{C}_\Theta(\rho) \equiv \prod_\sigma \mathcal{C}_\Theta(\sigma)^{\mathrm{rk}_\sigma(E/F)} \mod \mathbb{Q}^{\times 2}.$$

In other words, the p-parts of the left-hand side determine the parities of specific ranks: for any $\tau_p \in \mathbf{T}_{\Theta,p}$,

$$\prod_i (C_{E/F^{H_i}})^{n_i} \equiv \prod_p p^{\langle \tau_p, E(F)\rangle} \mod \mathbb{Q}^{\times 2}.$$

The three procedures may be carried out without assuming that Ш is finite, at the expense of working with Selmer groups rather than Mordell-Weil groups. In the first two cases, the outcome is

$$\begin{aligned} &\dim \mathcal{X}_p(E/K) &&\equiv \mathrm{ord}_p \frac{C_{E/K}}{C_{E'/K}} \mod 2 && \text{(isogeny)},\\ &\dim \mathcal{X}_2(E/K(\sqrt{d})) &&\equiv \mathrm{ord}_2 \frac{C_{E/K}C_{E_d/K}}{C_{E/K(\sqrt{d})}} \left|\frac{\Delta_{K(\sqrt{d})}^{1/2}}{\Delta_K}\right| \mod 2 && \text{(quad. twist)}. \end{aligned}$$

In the case of G-relations, according to [7] Thms. 1.1, 1.5, we have

Theorem 1.14. *Let F/K be a Galois extension of number fields with Galois group G. Let p be a prime and $\Theta = \sum n_i H_i$ a G-relation. For every elliptic curve E/K, the $\mathbb{Q}_pG$-representation $\mathcal{X}_p(E/F)$ is self-dual, and*

$$\langle \tau, \mathcal{X}_p(E/F)\rangle \equiv \mathrm{ord}_p \prod_i (C_{E/F^{H_i}})^{n_i} \mod 2 \qquad \textit{for all } \tau \in \mathbf{T}_{\Theta,p}.$$

The same is true for principally polarised abelian varieties A/K, except that when $p = 2$ we require that the polarisation comes from a K-rational divisor.

Remark 1.15. In contrast to Theorem 1.6, this result has no constraints on the reduction types of the abelian variety. So it always gives an expression for $\langle \tau, \mathcal{X}_p(A/F)\rangle$ for $\tau \in \mathbf{T}_{\Theta,p}$ in terms of local data.

Example 1.16. As in Example 1.9, suppose $\mathrm{Gal}(F/K) = \mathrm{D}_{2p^n}$. Then for a faithful 2-dimensional representation τ, the parity of $\langle \mathbf{1}\oplus\epsilon\oplus\tau, \mathcal{X}_p(A/F)\rangle$ is determined by local Tamagawa numbers, as $\mathrm{ord}_p C_{A/F}/C_{A/F^{\mathrm{C}_p}} \mod 2$. (Mazur and Rubin have another local expression for *precisely* the same parity; see [20] Thm. A.)

1.v. **Root numbers and Tamagawa numbers.** We have explained how in three situations (p-isogeny, quadratic twist, G-relations) the parity of some Selmer rank can be expressed in terms of *local* Tamagawa numbers. As root numbers are also products of *local* root numbers, this suggests a proof of the corresponding case of the parity conjecture by a place-by-place comparison (cf. [3, 5] for the isogeny case and [18, 19] for quadratic twists).

There are two subtle points:

First, the local terms do not always agree. In each case, one needs a good expression for the root numbers, separating the part that does agree with C_v and an "error term" that provably dies after taking the product over all places. This error term in the isogeny case is an Artin symbol ([3] Thm. 2.7, [5] Thms. 3, 4), for quadratic twists it is a Legendre symbol ([19] p. 307), and in our case it comes out as the local root number $w(\tau)^{2\dim A}$ (see Theorem 3.2). In fact, for group-theoretic reasons this contribution is trivial (Lemma A.1 and Theorem 2.56(1)), so here the local terms *do* agree.

Second, although the remaining compatibility of the corrected local root number and C_v is a genuinely local problem, they are computed for completely different objects — for instance in Example 1.16 the representation $\mathbf{1}\oplus\epsilon\oplus\tau$ bears little resemblance to $C_{E/F}/C_{E/F^{C_p}}$. In the isogeny and quadratic twist cases, the proof of this compatibility in [3, 5, 18] boils down to brutally working out an explicit formula for each term separately. That the two formulae then agree comes out as a miracle. In our case, for a *fixed* Galois group G and relation Θ this strategy works equally brutally, cf. [6] Prop. 3.3 for $G=\left(\begin{smallmatrix}1 & *\\ 0 & *\end{smallmatrix}\right)\subset \mathrm{GL}_2(\mathbb{F}_p)$.

The general case occupies §3 and relies on the theory of G-relations and regulator constants from §2. We first reduce our "semilocal" problem (places can split in F/K) to one about abelian varieties over local fields. If now A/K is an abelian variety over a *local* field, in all cases covered by Theorem 1.6 there is an explicit $\lambda=\pm1$ and a $\mathrm{Gal}(\bar K/K)$-module V such that

$$w(A/K,\tau)=w(\tau)^{2\dim A}\,\lambda^{\dim\tau}\,(-1)^{\langle\tau,V\rangle}$$

for all self-dual τ (see Table 3.9). For instance, when A is semistable, $\lambda=1$ and $V=X(\mathcal{T}^*)\otimes\mathbb{Q}$ is the character group of the toric part of the reduction of the dual abelian variety (Proposition 3.26). The compatibility statement reduces to proving that the function $\frac{\mathfrak{D}_V}{C_v}$ to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is representation-theoretic in the sense of §1.ii (cf. Theorem 3.2).

Let us note here that the statement of Theorem 1.14 is that $\mathfrak{D}_{\mathcal{X}_p}/\prod C_v$ is representation-theoretic. Thus V plays the rôle of a "local version" of the Selmer module $\mathcal{X}_p(A/F)$. Curiously, V is a rational representation, which is only conjecturally true of the Selmer module.

Example 1.17. Take $K=\mathbb{Q}_p$ for an odd prime p, and E/K an elliptic curve with non-split multiplicative reduction of type I_n. In this case the module V that computes root numbers is the 1-dimensional unramified character of

order 2. Let us consider $\mathfrak{D}_V$ and C_v ($=c_v$, the local Tamagawa number) in the unique $\mathrm{C}_2 \times \mathrm{C}_2$ extension of $\mathbb{Q}_p$:

$$
\begin{tikzcd}[column sep=small]
 & 2n \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & & & \mathbb{Q}_p(\sqrt{u},\sqrt{p}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & & & d \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
n \arrow[dr, dash] & 2 \arrow[d, dash] & 2 \arrow[dl, dash] & \xleftarrow{\ C_v\ } & \mathbb{Q}_p(\sqrt{u}) \arrow[dr, dash] & \mathbb{Q}_p(\sqrt{up}) \arrow[d, dash] & \mathbb{Q}_p(\sqrt{p}) \arrow[dl, dash] & \xmapsto{\ \mathfrak{D}_V\ } & \frac{d}{2} \arrow[dr, dash] & 1 \arrow[d, dash] & 1 \arrow[dl, dash] \\
 & 1 \text{ or } 2 & & & & \mathbb{Q}_p & & & & 1 &
\end{tikzcd}
$$

Here $\mathbb{Q}_p(\sqrt{u})$ is the quadratic unramified extension of $\mathbb{Q}_p$, and E has split multiplicative reduction precisely in those fields that contain it; d is the determinant of a fixed pairing on V, used in the definition of $\mathfrak{D}_V$. The group $\mathrm{C}_2 \times \mathrm{C}_2$ has up to multiples just one relation (see Example 2.3),

$$\Theta = \{1\} - \mathrm{C}_2^a - \mathrm{C}_2^b - \mathrm{C}_2^c + 2\,\mathrm{C}_2 \times \mathrm{C}_2.$$

The corresponding values of C_v and $\mathfrak{D}_V$ are

$$C_v(\Theta) = \frac{2n \cdot (1 \text{ or } 2)^2}{n \cdot 2 \cdot 2} = 2 \cdot \square \qquad\qquad \mathfrak{D}_V(\Theta) = \frac{d \cdot 1^2}{\frac{d}{2} \cdot 1 \cdot 1} = 2\,,$$

and so $\frac{C_v}{\mathfrak{D}_V}$ is representation theoretic (modulo squares!), by inspection.

This example explains our need to understand G-relations, behaviour of functions and $\mathfrak{D}_\rho$. To establish the compatibility of local root numbers and Tamagawa numbers in arbitrary extensions (Theorem 3.2), even for elliptic curves with non-split multiplicative reduction, requires the full force of the machinery of §2.

1.vi. **Notation.** For an abelian variety A/K we use the following notation:

$\mathcal{X}_p(A/F)$	$\mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim \mathrm{Sel}_{p^n}(A/F), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p$, the dual p^∞-Selmer.
$w(A/K)$	local root number of A/K for K local, or global root number, $\prod_v w(A/K_v)$ for K a number field.
$w(A/K,\tau)$	(local/global) root number for the twist of A by τ, see [30].
$c_v(A/K)$	local Tamagawa number of A at a finite place v of K (when K is local, the subscript v is purely decorational).
$C_v(A/K,\omega)$	$c_v(A/K)\cdot\lvert\omega/\omega^o\rvert_K$ for K non-Archimedean, where $\lvert\cdot\rvert_K$ is the normalised absolute value, and ω^o a Néron differential; $\int_{A(K)}\lvert\omega\rvert$ for $K=\mathbb{R}$; $2\int_{A(K)}\omega\wedge\bar{\omega}$ for $K=\mathbb{C}$. (K local; ω is a non-zero regular exterior form on A/K.)
$C_{A/K}$	$\prod_v C_v(A/K_v,\omega)$ for any global non-zero regular exterior form ω; independent of ω (product formula).

Notation for representations $G \to \mathrm{GL}_n(\mathcal{K})$, $\mathcal{K}$ a field of characteristic 0: $\langle,\rangle_G$, $\langle,\rangle$ usual inner product of two characters of representations; $\mathcal{K}[G]$ regular representation; $\mathcal{K}[G/H]$ permutation representation of G on the left cosets of H; $\mathbf{1}$ trivial representation; τ^* contragredient representation; ρ^H the H-invariants of ρ. We call ρ self-dual if $\rho \cong \rho^*$, equivalently $\rho\otimes\bar{\mathcal{K}} \cong \rho^*\otimes\bar{\mathcal{K}}$.

For a $\mathcal{K}$-vector space V and a non-degenerate $\mathcal{K}$-bilinear pairing $\langle,\rangle$ with values in $\mathcal{L} \supset \mathcal{K}$, we write $\det(\langle,\rangle|V) \in \mathcal{L}^\times/\mathcal{K}^{\times 2}$ for $\det(\langle e_i, e_j\rangle_{i,j})$ in any $\mathcal{K}$-basis $\{e_i\}$ of V.

For functions on subgroups of G we use the following notation:

Θ	a G-relation $\sum_i n_i H_i$ between permutation representations, i.e. $\sum_i \mathbb{C}[G/H_i]^{\oplus n_i} = 0$, see Definition 2.1.
$\mathcal{C}_\Theta(\rho)$	regulator constant for a G-representation ρ, see Definition 2.13.
$\varphi(\Theta)$	$\prod_i \varphi(H_i)^{n_i}$ for $\Theta = \sum_i n_i H_i$, see §2.iii.
$\varphi \sim \psi$	equivalence relation $\varphi(\Theta)=\psi(\Theta)$ for all G-relations Θ, see §2.iii.
$\mathfrak{D}_\rho$	$H \mapsto \det(\frac{1}{\lvert H\rvert}\langle,\rangle\lvert\rho^H)$, see Definition 2.40.
$(\cdots)$	see Definitions 2.33, 2.35.

D_{2n} denotes the dihedral group of order $2n$ (including $C_2 \times C_2$ for $n = 2$). Conjugation of subgroups is usually written as a superscript, $H^x = xHx^{-1}$.

By a local field we mean a finite extension of $\mathbb{Q}_p, \mathbb{R}$ or $\mathbb{F}_p((t))$ (the latter will never occur). We write $e_{M/L}, f_{M/L}$ for the ramification degree and the residue degree of an extension M/L of local fields, μ_n for the set of n^{th} roots of unity and ord_p for the p-valuation of a rational or a p-adic number.

2. Functions on the Burnside ring

This section is dedicated to relations between permutation representations, behaviour of functions on the Burnside ring with respect to such relations, the issue whether a function is representation-theoretic, and regulator constants. As explained in the introduction, the applications we have in mind relate to elliptic curves and abelian varieties. On the other hand, the results are self-contained, purely group-theoretic in nature, and they may be of independent interest.

Throughout the section G is an abstract finite group.

2.i. Relations between permutation representations.

Let G be a finite group and S the set of subgroups of G up to conjugacy. By abuse of notation, for a subgroup $H < G$ we also write H for its class in S. The *Burnside ring* of G is the free abelian group $\mathbb{Z}S$ (we will not use its multiplicative structure). The elements of S are in one-to-one correspondence with transitive G-sets via $H \mapsto G/H$. This extends to a correspondence between elements of $\mathbb{Z}S$ with non-negative coefficients and finite G-sets, under which addition translates to disjoint union.

The map $H \mapsto \mathbb{C}[G/H] (\cong \text{Ind}_H^G \mathbf{1}_H)$ defines a ring homomorphism from the Burnside ring to the representation ring of G. On the level of G-sets, this map is simply $X \mapsto \mathbb{C}[X]$. Here in §2.i we consider its kernel:

Definition 2.1. We call an element of the Burnside ring of G

$$\Theta = \sum\nolimits_i n_i H_i \qquad (n_i \in \mathbb{Z},\ H_i < G)$$

a *relation between permutation representations of* G or simply a *G-relation* if $\oplus_i \mathbb{C}[G/H_i]^{\oplus n_i} = 0$ as a virtual representation, i.e. the character $\sum_i n_i \chi_{\mathbb{C}[G/H_i]}$ is zero. In other words, if Θ corresponds to a formal difference of two G-sets, we require that they have isomorphic permutation representations.

Exercise 2.2. A cyclic group C_n has no non-trivial relations.

Example 2.3. The group $G=\mathrm{C}_2\times\mathrm{C}_2$ has five subgroups $\{1\}$, C_2^a, C_2^b, C_2^c, G and four irreducible representations $\mathbf{1}, \epsilon^a, \epsilon^b, \epsilon^c$. Writing out the permutation representations,

$$\mathbb{C}[G]\cong\mathbf{1}\oplus\epsilon^a\oplus\epsilon^b\oplus\epsilon^c,\quad \mathbb{C}[G/\mathrm{C}_2^a]\cong\mathbf{1}\oplus\epsilon^a,\quad \mathbb{C}[G/\mathrm{C}_2^b]\cong\mathbf{1}\oplus\epsilon^b,\quad \mathbb{C}[G/\mathrm{C}_2^c]\cong\mathbf{1}\oplus\epsilon^c,\quad \mathbf{1}\cong\mathbf{1},$$

we see that, up to multiples, there is a unique G-relation

$$\Theta = \{1\} - \mathrm{C}_2^a - \mathrm{C}_2^b - \mathrm{C}_2^c + 2\,G.$$

Example 2.4. Generally, any dihedral group $G = \mathrm{D}_{2n}$ with presentation $\langle g,h|h^n=g^2=(gh)^2=1\rangle$ has the relation

$$\{1\} - \langle g\rangle - \langle gh\rangle - \langle h\rangle + 2\,G.$$

When n is odd it can be written as $\{1\}-2\,\mathrm{C}_2-\mathrm{C}_n+2\,\mathrm{D}_{2n}$, and it is unique up to multiples when n is prime. For D_8 and D_{12}, together with

$$\mathrm{D}_8 \begin{cases} \langle g\rangle-\langle gh\rangle-\langle g,h^2\rangle+\langle gh,h^2\rangle \\ \{1\}-\langle h^2\rangle-2\langle g\rangle+2\langle gh,h^2\rangle \end{cases} \qquad \mathrm{D}_{12} \begin{cases} \langle h^3\rangle-\langle h\rangle-2\langle g,h^3\rangle+2G \\ \langle h^2\rangle-\langle h\rangle-\langle gh,h^2\rangle-\langle g,h^2\rangle+2G \\ \langle g\rangle-\langle gh\rangle+\langle gh,h^2\rangle-\langle g,h^2\rangle \end{cases}$$

it forms a $\mathbb{Z}$-basis of all G-relations (cf. Table 3.14 for the lattice of these subgroups.)

Remark 2.5. The number of irreducible $\mathbb{Q}G$-representations coincides with the number of cyclic subgroups of G up to conjugacy ([36] §13.1, Cor. 1). If G is not cyclic, this is clearly less than the number of all subgroups up to conjugacy, so the map $\sum n_iH_i \mapsto \oplus\mathbb{C}[G/H_i]^{\oplus n_i}$ must have a kernel. Hence every non-cyclic group has non-trivial relations.

Example 2.6 (Artin formalism)**.** Let F/K be a Galois extension of number fields with Galois group G. For $H<G$, the Dedekind ζ-function $\zeta_{F^H}(s)$ agrees with the L-function over K of the Artin representation $\mathbb{C}[G/H]$. So a G-relation $\sum_i n_iH_i$ yields the identity

$$\prod_i \zeta_{F^{H_i}}(s)^{n_i} = 1.$$

Similarly, if E/K is an elliptic curve (or an abelian variety),

$$\prod_i L(E/F^{H_i},s)^{n_i} = 1.$$

Notation 2.7. For $D<G$, define a map Res_D from the Burnside ring of G to that of D, and a map Ind_D^G in the opposite direction by

$$\mathrm{Res}_D\, H = \sum_{x\in H\backslash G/D} D\cap H^{x^{-1}} \qquad \text{and} \qquad \mathrm{Ind}_D^G\, H = H\,.$$

On the level of representations (i.e. under $H\mapsto\mathbb{C}[G/H]$), these are the usual restriction and induction. On the level of G-sets, Res_D simply restricts the action from G to D (Mackey's decomposition).

Theorem 2.8. *Suppose $D, H_i < G$, $N \lhd G$.*

1. *The sum and the difference of two G-relations is a G-relation.*
2. *If $\Theta = \sum_i n_i H_i$ and $m\Theta$ is a G-relation, then Θ is a G-relation.*
3. *(lifting) If $H_i \supset N$ and $\sum_i n_i H_i N/N$ is a G/N-relation, then $\sum_i n_i H_i$ is a G-relation.*
4. *(induction) Any D-relation is also a G-relation; i.e. if $\Theta = \sum_i n_i H_i$ is a D-relation, then $\mathrm{Ind}_D^G \Theta = \sum_i n_i H_i$ is a G-relation.*
5. *(projection) If $\sum_i n_i H_i$ is a G-relation, then $\sum_i n_i H_i N/N$ is a G/N-relation.*
6. *(restriction) If $\Theta = \sum_i n_i H_i$ is a G-relation, then its restriction $\mathrm{Res}_D \Theta = \sum_i n_i \sum_{x \in H_i \backslash G/D} D \cap H_i^{x^{-1}}$ is a D-relation.*

Proof. (1),(2),(3) Clear. (4) Induction is transitive. (5) This follows from the fact that $\mathbb{C}[G/H_i]^N \cong \mathbb{C}[G/NH_i]$ as a G-representation. (The invariants $\mathbb{C}[G/H]^N$ come from orbits of N on G/H, so this space has a basis $\{\sum_{x\in\Delta} xH\}_\Delta$ with Δ ranging over the double cosets $N\backslash G/H$ ($=G/NH$). As N is normal, G permutes the basis elements, and this is the same as the action on G/NH.) (6) This is a consequence of Mackey's formula, $\mathrm{Res}_D \mathbb{C}[G/H] \cong \oplus_{x\in H\backslash G/D} \mathbb{C}[D/D\cap H^{x^{-1}}]$. □

Properties (3) and (4) allow one to lift relations from quotient groups and induce them from subgroups. This is not to suggest that relations can always be built up like that, for instance dihedral groups have relations while cyclic groups do not. Here is a case when this does work:

Lemma 2.9. *Let $D \lhd G$, and suppose that G acts on the Burnside ring of D by conjugation through a quotient of order n.*

1. *If $\Theta = \sum_i n_i H_i$ is a G-relation with $H_i \subset D$, then $n\Theta$ is induced from a D-relation.*
2. *Suppose that $N \lhd G$ with $N \subset D$, and that each subgroup of G either contains N or is contained in D. Then for every G-relation Θ, $n\Theta$ is a sum of a relation induced from D and one lifted from G/N.*

Proof. (1) Let G_0 be the kernel of the action of G on the Burnside ring of D. As a G-relation, we may write $n\Theta$ as

$$n\Theta = \sum_i n_i \Big(\sum_{g\in G/G_0} gH_ig^{-1} \Big).$$

We claim that in this form it is a D-relation. Indeed, restricting it to D, on the one hand, yields a D-relation (Theorem 2.8(6)) and, on the other hand, multiplies the expression by $[G:D]$. Hence the expression itself is a D-relation.

(2) If Θ is a G-relation, write it as $\sum_i n_i H_i + \sum_j n'_j H'_j$ with $H_i \supset N$ and $H'_j \subset D$. Then

$$\Theta = (\textstyle\sum_i n_i H_i + \sum_j n'_j NH'_j) + (\sum_j n'_j H'_j - \sum_j n'_j NH'_j).$$

The first term is a relation lifted from G/N (Theorem 2.8(5)), and the second term is therefore a G-relation with constituents in D, so (1) applies. $\square$

Example 2.10. Suppose $G = \mathrm{C}_{u2^m} \times \mathrm{C}_{2^k}$ with u odd and $k > m$. Set

$$G_1 = \{1\} \times \mathrm{C}_{2^{k-m}} \;\subset\; G_2 = \mathrm{C}_{u2^m} \times \mathrm{C}_{2^{k-1}} \;\subset\; G, \qquad G/G_1 \cong \mathrm{C}_{u2^m} \times \mathrm{C}_{2^m}.$$

Every element outside G_2 generates a subgroup containing G_1, so every subgroup not in G_2 contains G_1. Since every subgroup of G is normal, Lemma 2.9(2) shows that every G-relation is a sum of a relation coming from G_2 and one lifted from G/G_1. By induction, the lattice of G-relations is generated by ones coming from subquotients $\mathrm{C}_{u2^m} \times \mathrm{C}_{2^t} \,/\, \{1\} \times \mathrm{C}_{2^{t-m}}$ for $m \le t \le k$, all isomorphic to $\mathrm{C}_u \times \mathrm{C}_{2^m} \times \mathrm{C}_{2^m}$.

Example 2.11. Suppose $G = \langle x, y \,|\, x^n = y^{2^k} = 1, yxy^{-1} = x^{-1} \rangle$, a semi-direct product of C_{2^k} by C_n for some $k, n \ge 1$. Consider

$$G_1 = \langle y^2 \rangle \subset G_2 = \langle x, y^2 \rangle \subset G, \qquad G/G_1 \cong \mathrm{D}_{2n},\; G/G_2 \cong \mathrm{C}_2.$$

Note that if $x^a y^b \in H < G$ with b odd, then $(x^a y^b)^2 = y^{2b} \in H$ implies that $H \supset G_1$. Equivalently, every subgroup not contained in G_2 contains G_1. By Lemma 2.9(2), if Θ is any G-relation, then 2Θ is a sum of a relation induced from G_2 and one lifted from G/G_1. If $4 \nmid n$, it is easy to verify that every subgroup of G_2 is normal in G, so Θ itself is already of this form.

Observe that $G_2 \cong \mathrm{C}_n \times \mathrm{C}_{2^{k-1}}$, whose relations were discussed in the previous example.

2.ii. **Regulator constants.** Let $\mathcal{K}$ be a field of characteristic 0. In this section we define regulator constants for self-dual $\mathcal{K}G$-representations, first introduced in [6] for $\mathcal{K} = \mathbb{Q}$. (The name "regulator constant" comes from regulators of elliptic curves; see §1.iv.)

Notation 2.12. Suppose V is a $\mathcal{K}$-vector space with a non-degenerate $\mathcal{K}$-bilinear pairing $\langle , \rangle$ that takes values in some extension $\mathcal{L}$ of $\mathcal{K}$. We write $\det(\langle , \rangle | V) \in \mathcal{L}^\times / \mathcal{K}^{\times 2}$ for $\det(\langle e_i, e_j \rangle_{i,j})$ in any $\mathcal{K}$-basis $\{e_i\}$ of V.

Definition 2.13. Let G be a finite group, ρ a self-dual $\mathcal{K}G$-representation, and $\Theta = \sum_i n_i H_i$ a G-relation. Pick a G-invariant non-degenerate $\mathcal{K}$-bilinear pairing $\langle , \rangle$ on ρ with values in some extension $\mathcal{L}$ of $\mathcal{K}$, and define the *regulator constant*

$$\mathcal{C}_\Theta(\rho) = \mathcal{C}_\Theta^{\mathcal{K}}(\rho) = \prod_i \det\bigl(\tfrac{1}{|H_i|}\langle , \rangle | \rho^{H_i}\bigr)^{n_i} \in \mathcal{K}^\times / \mathcal{K}^{\times 2}.$$

(This is well-defined, non-zero and independent of $\langle , \rangle$ by Lemma 2.15 and Theorem 2.17. It follows that it lies in $\mathcal{K}^\times/\mathcal{K}^{\times 2}$ rather than $\mathcal{L}^\times/\mathcal{K}^{\times 2}$ as the pairing can be chosen to be $\mathcal{K}$-valued.)

Exercise 2.14. Let $G = \mathrm{C}_2 \times \mathrm{C}_2$ and $\Theta = \{1\} - \mathrm{C}_2^a - \mathrm{C}_2^b - \mathrm{C}_2^c + 2\,G$ from Example 2.3. Then $\mathcal{C}_\Theta(\chi) = 2$ for all four 1-dimensional characters χ of G.

Lemma 2.15. *Suppose ρ is a $\mathcal{K}G$-representation, and $\langle,\rangle$ a G-invariant $\mathcal{K}$-bilinear non-degenerate pairing on ρ. For every $H<G$, the restriction of $\langle,\rangle$ to ρ^H is non-degenerate. In other words,* $\det(\langle,\rangle|\rho^H)\neq 0$.

Proof. Consider the projection $P:\rho\to\rho^H$ given by $v\mapsto\frac{1}{|H|}\sum_{h\in H}h\cdot v$. Then $\rho=\rho^H\oplus\ker P$, and for $v\in\rho^H, w\in\ker P$,

$$\langle v,w\rangle=\frac{1}{|H|}\sum_{h\in H}\langle hv,hw\rangle=\langle v,P(w)\rangle=0.$$

So ρ^H and $\ker P$ are orthogonal to each other, and the pairing cannot be degenerate on either of them. $\square$

Lemma 2.16. *Let $\Theta=\sum_i n_iH_i$ be a G-relation and ρ a $\mathcal{K}G$-representation. Then*

$$\sum\nolimits_i n_i\dim\rho^{H_i}=0.$$

Proof. By Frobenius reciprocity,

$$\begin{aligned}\sum n_i\dim\rho^{H_i}&=\sum n_i\,\langle\mathrm{Res}_{H_i}\rho,\mathbf{1}_{H_i}\rangle_{H_i}=\sum n_i\langle\rho,\mathrm{Ind}_{H_i}^G\mathbf{1}_{H_i}\rangle_G\\&=\langle\rho,\oplus(\mathrm{Ind}_{H_i}^G\mathbf{1}_{H_i})^{\oplus n_i}\rangle_G=\langle\rho,0\rangle_G=0.\end{aligned}$$ $\square$

We now prove that regulator constants are independent of the pairing:

Theorem 2.17. *Let $\Theta=\sum_i n_iH_i$ be a G-relation, ρ a self-dual $\mathcal{K}G$-representation, and $\langle,\rangle_1,\langle,\rangle_2$ two non-degenerate G-invariant $\mathcal{K}$-bilinear pairings on ρ. Computing the determinants with respect to the same bases of ρ^{H_i} on both sides,*

$$\prod_i\det(\tfrac{1}{|H_i|}\langle,\rangle_1|\rho^{H_i})^{n_i}=\prod_i\det(\tfrac{1}{|H_i|}\langle,\rangle_2|\rho^{H_i})^{n_i}.$$

(This is an actual equality, not modulo $\mathcal{K}^{\times 2}$.)

Proof. We may assume $\mathcal{K}$ is algebraically closed. It is enough to prove the statement for a particular choice of bases of ρ^{H_i}, as seen from the transformation rule $X\mapsto M^tXM$ for matrices of bilinear forms under change of basis.

If $\rho=\alpha\oplus\beta$ with α,β self-dual and $\mathrm{Hom}_G(\alpha,\beta^*)=0$, then $\langle a,b\rangle_1=0$ for $a\in\alpha$ and $b\in\beta$, and similarly for $\langle,\rangle_2$. Since $\rho^H=\alpha^H\oplus\beta^H$, choosing bases that respect the decomposition reduces the problem to α and β separately. Thus, we may assume that either $\rho=\tau^{\oplus n}$ with τ irreducible and self-dual, or $\rho=\sigma^{\oplus n}\oplus(\sigma^*)^{\oplus n}$ with σ irreducible and not self-dual.

In the first case, for each H_i fix a basis of τ^{H_i} and take the induced bases of $(\tau^{H_i})^{\oplus n}=\rho^{H_i}$. Let $\langle,\rangle_\tau$ be a non-degenerate G-invariant bilinear pairing on τ, and let M_i be its matrix on the chosen basis of τ^{H_i}. As $\langle,\rangle_\tau$ is unique up to scalar ($\mathcal{K}$ is algebraically closed), the matrix of $\langle,\rangle_1$ on ρ^{H_i} is

$$T(\Lambda,M_i)=\begin{pmatrix}\lambda_{11}M_i&\lambda_{12}M_i&\dots&\lambda_{1n}M_i\\\lambda_{21}M_i&\lambda_{22}M_i&\dots&\lambda_{2n}M_i\\\vdots&\vdots&\ddots&\vdots\\\lambda_{n1}M_i&\lambda_{n2}M_i&\dots&\lambda_{nn}M_i\end{pmatrix},$$

for some $n\times n$ matrix $\Lambda=(\lambda_{xy})$ not depending on H_i. Hence

$$\det(\tfrac{1}{|H_i|}\langle,\rangle_1|\rho^{H_i})=(\det\Lambda)^{\dim\tau^{H_i}}(\det\tfrac{1}{|H_i|}M_i)^n\,.$$

The dimensions $\dim\tau^{H_i}$ cancel in Θ by Lemma 2.16, so $\prod_i\det(\frac{1}{|H_i|}\langle,\rangle_1|\rho^{H_i})^{n_i}$ does not depend on Λ, and takes therefore the same value for $\langle,\rangle_2$.

The argument in the second case is similar. The matrix of $\langle,\rangle_1$ on ρ^{H_i} is of the form $\left(\begin{smallmatrix}0 & T(\Lambda,M_i)\\ T(\Lambda',M_i') & 0\end{smallmatrix}\right)$ where M_i and M_i' are the matrices of a fixed G-invariant non-degenerate pairing $\langle,\rangle_\sigma:\sigma\times\sigma^*\to\mathcal{K}$ and its transpose. Again the contributions $((-1)^n\det\Lambda\det\Lambda')^{\dim\tau^{H_i}}$ cancel in Θ and the result follows. $\square$

Corollary 2.18. *Regulator constants are multiplicative in Θ and ρ,*

$$\mathcal{C}_{\Theta_1+\Theta_2}(\rho)=\mathcal{C}_{\Theta_1}(\rho)\mathcal{C}_{\Theta_2}(\rho),$$
$$\mathcal{C}_{\Theta}(\rho_1\oplus\rho_2)=\mathcal{C}_{\Theta}(\rho_1)\mathcal{C}_{\Theta}(\rho_2).$$

If $\mathcal{L}\supset\mathcal{K}$, then $\mathcal{C}^{\mathcal{K}}_\Theta(\rho)=\mathcal{C}^{\mathcal{L}}_\Theta(\rho\otimes\mathcal{L})$ in $\mathcal{L}^\times/\mathcal{L}^{\times 2}$.

Example 2.19. Suppose $\rho=\mathcal{K}[G/D]$ for some subgroup D of G. Take the standard pairing on ρ, making the elements of G/D an orthonormal basis. The space of invariants ρ^H has a basis consisting of H-orbit sums of these basis vectors. Since $\det(\langle,\rangle|\rho^H)$ is the product of lengths of these orbits,

$$\det(\tfrac{1}{|H|}\langle,\rangle|\rho^H)=\prod_{w\in H\backslash G/D}\tfrac{1}{|H|}\tfrac{|HwD|}{|D|}=\prod_{w\in H\backslash G/D}\tfrac{1}{|H\cap D^w|}\,,$$

which yields an elementary formula for the regulator constants of ρ. Note that for many groups, every $\mathcal{K}G$-representation is a $\mathbb{Z}$-linear combinations of such ρ, e.g. dihedral groups D_{2p^n} when $\mathcal{K}=\mathbb{Q}$ or $\mathbb{Q}_p$, or symmetric groups.

Example 2.20. For an odd prime p, the dihedral group $G=\mathrm{D}_{2p}$ has the relation (cf. Example 2.4)

$$\Theta=\{1\}-\ 2\mathrm{C}_2-\mathrm{C}_p+2\,G.$$

For $\mathcal{K}=\mathbb{Q}$ or $\mathbb{Q}_p$, the irreducible $\mathcal{K}G$-representations are $\mathbf{1}$, sign ϵ and $(p-1)$-dimensional ρ. Writing them as combinations of permutation representations $\mathcal{K}[G/H]=\mathrm{Ind}_H^G\mathbf{1}_H$, we can compute their regulator constants as in Example 2.19: modulo squares,

$$\begin{array}{lclcll}
\mathcal{C}_\Theta(\mathbf{1}) & = & \mathcal{C}_\Theta(\mathrm{Ind}_G^G\mathbf{1}) & = & (\frac{1}{1})^1(\frac{1}{2})^{-2}(\frac{1}{p})^{-1}(\frac{1}{2p})^2 & \equiv p\\
\mathcal{C}_\Theta(\mathbf{1})\mathcal{C}_\Theta(\epsilon) & = & \mathcal{C}_\Theta(\mathrm{Ind}_{\mathrm{C}_p}^G\mathbf{1}) & = & (\frac{1}{1^2})^1(\frac{1}{1})^{-2}(\frac{1}{p^2})^{-1}(\frac{1}{p})^2 & \equiv 1\\
\mathcal{C}_\Theta(\mathbf{1})\mathcal{C}_\Theta(\rho) & = & \mathcal{C}_\Theta(\mathrm{Ind}_{\mathrm{C}_2}^G\mathbf{1}) & = & (\frac{1}{1^p})^1(\frac{1}{2\cdot 1^{(p-1)/2}})^{-2}(\frac{1}{1})^{-1}(\frac{1}{2})^2 & \equiv 1.
\end{array}$$

So $\mathcal{C}_\Theta(\mathbf{1})=\mathcal{C}_\Theta(\epsilon)=\mathcal{C}_\Theta(\rho)=p$.

Example 2.21 (D_{2p^n}, p odd, $\mathcal{K}=\mathbb{Q}_p$)**.** Generally, suppose $G=\mathrm{D}_{2p^n}$ with p odd, and consider the G-relations coming from various D_{2p} subquotients,

$$\Theta_{n+1-k}=\mathrm{C}_{p^{k-1}}-2\,\mathrm{D}_{2p^{k-1}}-\mathrm{C}_{p^k}+2\,\mathrm{D}_{2p^k}\qquad(1\le k\le n).$$

The irreducible $\mathbb{Q}_pG$-representations are $\mathbf{1}$, sign ϵ and ρ_k of dimension $p^k - p^{k-1}$ for $1 \le k \le n$. A computation as in Example 2.20 shows that

$$\mathcal{C}_{\Theta_k}(\mathbf{1}) = \mathcal{C}_{\Theta_k}(\epsilon) = \mathcal{C}_{\Theta_k}(\rho_k) = p, \qquad \mathcal{C}_{\Theta_k}(\rho_j) = 1 \text{ for } j \ne k.$$

Example 2.22 ($\mathrm{D}_{2p^n}, p{=}2, \mathcal{K}{=}\mathbb{Q}_2$)**.** For $G{=}\mathrm{D}_{2^{n+1}}$ consider the G-relations

$$\begin{array}{lcll} \Theta_1 & = & \mathrm{C}_{2^{n-1}} - \mathrm{D}^a_{2^n} - \mathrm{D}^b_{2^n} - \mathrm{C}_{2^n} + 2\,G & \\ \Theta_{n+1-k} & = & \mathrm{D}^a_{2^k} - \mathrm{D}^b_{2^k} - \mathrm{D}^a_{2^{k+1}} + \mathrm{D}^b_{2^{k+1}} & \qquad (1 \le k < n). \end{array}$$

Here $\mathrm{C}_{2^k} {=} \langle h^{2^{n-k}} \rangle$, $\mathrm{D}^a_{2^k} {=} \langle h^{2^{n-k}}, g \rangle$, $\mathrm{D}^b_{2^k} {=} \langle h^{2^{n-k}}, gh \rangle$ in terms of the generators given in Example 2.4. In this case, the irreducible $\mathbb{Q}_2G$-representations are $\mathbf{1}$ (trivial), ρ_k of dimension $2^k {-} 2^{k-1}$ for $2 \le k \le n$, and one-dimensional characters $\epsilon, \epsilon^a, \epsilon^b$ that factor through G/C_{2^n}, $G/\mathrm{D}^a_{2^{n-1}}$ and $G/\mathrm{D}^b_{2^{n-1}}$ respectively. The regulator constants are

$$\begin{array}{lll} \mathcal{C}_{\Theta_1}(\mathbf{1}) = \mathcal{C}_{\Theta_1}(\epsilon) = \mathcal{C}_{\Theta_1}(\epsilon^a) = \mathcal{C}_{\Theta_1}(\epsilon^b) & = 2, & \\ \mathcal{C}_{\Theta_k}(\epsilon^a) = \mathcal{C}_{\Theta_k}(\epsilon^b) = \mathcal{C}_{\Theta_k}(\rho_k) & = 2 & \qquad (k > 1), \end{array}$$

and trivial on other irreducibles.

Example 2.23. Let $G = \mathrm{SL}_2(\mathbb{F}_3)$, which is the semi-direct product of C_3 by the quaternion group Q_8. Denote its complex irreducible representations by $\mathbf{1}, \chi, \bar\chi$ (1-dim.), $\tau, \chi\tau, \bar\chi\tau$ (τ symplectic 2-dim.) and ρ (3-dim.). A basis of G-relations and their regulator constants for the $\mathbb{Q}G$-irreducibles are

	$\mathbf{1}$	$\chi \oplus \bar\chi$	ρ	$\tau^{\oplus 2}$	$\chi\tau \oplus \bar\chi\tau$
$\mathrm{C}_4 - \mathrm{C}_6 - \mathrm{Q}_8 + G$	2	1	2	1	1
$\mathrm{C}_2 - 3\mathrm{C}_4 + 2\mathrm{Q}_8$	2	1	2	1	1

The table stays the same if $\mathbb{Q}$ is replaced by any $\mathcal{K}$ of characteristic 0, except that τ may become realisable over $\mathcal{K}$, in which case $\mathcal{C}^{\mathcal{K}}_{\Theta}(\tau)$ and not just $\mathcal{C}^{\mathcal{K}}_{\Theta}(\tau^{\oplus 2})$ makes sense. This regulator constant will still be 1 by Corollary 2.25 below, because τ is symplectic. Observe that in the table the representations $V \oplus V^*$ also have trivial regulator constants, which is true for all groups by the same corollary.

Let us record a number of situations when the regulator constants are trivial; other properties are discussed in §2.iv. The following result, or rather Corollary 2.25, was motivated by the behaviour of root numbers of elliptic curves (see Proposition A.2).

Theorem 2.24. *Suppose ρ is a self-dual $\mathcal{K}G$-representation such that $\rho \otimes_{\mathcal{K}} \bar{\mathcal{K}}$ admits a non-degenerate alternating G-invariant pairing. Then $\mathcal{C}_\Theta(\rho) = 1$ for every G-relation Θ.*

Proof. Since $\dim \mathrm{Hom}_G(\mathbf{1}, \rho \wedge \rho)$ is the same over $\mathcal{K}$ and $\bar{\mathcal{K}}$, there is also a non-degenerate alternating G-invariant pairing $\langle , \rangle$ on ρ itself. By Lemma 2.15, its restriction to ρ^H is non-degenerate (and alternating) for every subgroup H of G. In an appropriate basis for ρ^H this pairing is given by a matrix $\left(\begin{smallmatrix} 0 & A \\ -A^t & 0 \end{smallmatrix}\right)$, so $\det(\frac{1}{|H|}\langle , \rangle | \rho^H)$ is a square in $\mathcal{K}$. $\square$

Corollary 2.25. *Let ρ be a self-dual $\mathcal{K}G$-representation. Suppose either*

(1) *ρ is symplectic as a $\bar{\mathcal{K}}$-representation, or*
(2) *$\rho \otimes \bar{\mathcal{K}} \cong \tau \oplus \tau$ for some $\bar{\mathcal{K}}G$-representation τ, or*
(3) *all $\bar{\mathcal{K}}$-irreducible constituents of $\rho \otimes \bar{\mathcal{K}}$ are not self-dual.*

Then $\mathcal{C}_\Theta(\rho) = 1$ for every G-relation Θ.

Proof. It suffices to check that in each case $\rho \otimes_{\mathcal{K}} \bar{\mathcal{K}}$ carries a non-degenerate alternating G-invariant pairing. This holds by definition in case (1). In cases (2) and (3), $\rho \otimes_{\mathcal{K}} \bar{\mathcal{K}}$ is of the form $V \oplus V^*$. Writing P for the matrix of the canonical map $V \times V^* \to \bar{\mathcal{K}}$, the pairing $\left(\begin{smallmatrix} 0 & P \\ -P^t & 0 \end{smallmatrix}\right)$ has the required properties. □

Lemma 2.26. *Let ρ be a self-dual $\mathcal{K}G$-representation. Suppose $\Theta = \sum n_i H_i$ is a G-relation such that no $\bar{\mathcal{K}}$-irreducible constituent of ρ occurs in any of the $\mathcal{K}[G/H_i]$. Then $\mathcal{C}_\Theta(\rho) = 1$.*

Proof. By Frobenius reciprocity, $\dim \rho^{H_i} = \langle \mathbf{1}, \mathrm{Res}_{H_i} \rho \rangle = \langle \mathcal{K}[G/H_i], \rho \rangle = 0$. □

Remark 2.27. Suppose R is a principal ideal domain whose field of fractions $\mathcal{K}$ has characteristic coprime to $|G|$. If ρ is a free R-module of finite rank with a G-action, then $\mathcal{C}_\Theta(\rho)$ may be defined in the same way,

$$\mathcal{C}_\Theta(\rho) = \prod\nolimits_i \det\left(\tfrac{1}{|H_i|}\langle,\rangle \middle| \rho^{H_i}\right)^{n_i} \in \mathcal{K}^\times / R^{\times 2},$$

where the determinants are now computed on R-bases of ρ^{H_i}. The pairing $\langle,\rangle$ may take values in any extension of $\mathcal{K}$ as before, and the class of $\mathcal{C}_\Theta(\rho)$ in $\mathcal{K}^\times/R^{\times 2}$ is independent of $\langle,\rangle$.

For instance, when $R = \mathbb{Z}$ the group $R^{\times 2}$ is trivial, so $\mathcal{C}_\Theta$ associates a well-defined rational number to every $\mathbb{Z}G$-lattice. Also, if R is a discrete valuation ring with maximal ideal $\mathfrak{m}$ and residue field $R/\mathfrak{m} = k$ with $\mathrm{char}\, k \nmid |G|$, it is not difficult to see that $\mathcal{C}_\Theta(\rho \otimes \mathcal{K})$ is in $R^\times/R^{\times 2}$, and

$$\mathcal{C}_\Theta(\rho \otimes \mathcal{K}) = \mathcal{C}_\Theta(\rho \otimes k) \mod \mathfrak{m}.$$

As every $\mathcal{K}G$-representation admits a G-invariant R-lattice, we deduce

Corollary 2.28. *Let $\mathcal{K} = \mathbb{Q}$ or $\mathcal{K} = \mathbb{Q}_p$, and let ρ be a $\mathcal{K}G$-representation. If $p \nmid |G|$, then $\mathrm{ord}_p\, \mathcal{C}_\Theta(\rho)$ is even for every G-relation Θ.*

2.iii. **Functions modulo G-relations.** We now turn to linear functions

$$\varphi: \text{ Burnside ring of } G \longrightarrow \underset{\text{(written multiplicatively)}}{\text{abelian group}}$$

or, equivalently, functions on G-sets that satisfy $\varphi(X \amalg Y) = \varphi(X)\varphi(Y)$. Our main concern is the distinction between functions that are representation-theoretic (i.e. only depend on $\mathbb{C}[X]$) and those that are not. We say that

- φ is *trivial* on an element Ψ of the Burnside ring of G if $\varphi(\Psi) = 1$.
- $\varphi \sim \varphi'$ if φ/φ' is trivial on all G-relations.

So, φ is representation-theoretic in the sense of §1.ii if and only if $\varphi \sim 1$.

Exercise 2.29. For a constant λ, the function $H \mapsto \lambda^{[G:H]} (= \lambda^{\dim \mathbb{C}[G/H]})$ to $\mathbb{R}^\times$ is trivial on G-relations. On the other hand, $H \mapsto |H|$ in general is not.

Example 2.30. The constant function $\varphi : H \mapsto \lambda$ is trivial on G-relations:

$$\varphi\bigl(\sum n_i H_i\bigr) = \prod \lambda^{n_i} = \prod \lambda^{n_i \langle \mathbf{1}, \mathbb{C}[G/H_i]\rangle} = \lambda^{\langle \mathbf{1}, \bigoplus \mathbb{C}[G/H_i]^{\oplus n_i}\rangle} = \lambda^0 = 1.$$

Example 2.31. A cyclic group has no relations, so $\varphi \sim 1$ for every φ.

Example 2.32. If E/K is an elliptic curve and $G = \mathrm{Gal}(F/K)$, then

$$\mathbf{L} : H \longmapsto L(E/F^H, s)$$

is a function with values in the multiplicative group of meromorphic functions on $\mathrm{Re}\, s > \frac{3}{2}$. By Artin formalism, $\mathbf{L} \sim 1$ (Example 2.6). As explained in §1.iv, the Birch–Swinnerton-Dyer conjecture implies that

$$C :\ H \longmapsto C_{E/F^H} \qquad \text{and} \qquad \mathrm{Reg} :\ H \longmapsto \mathrm{Reg}_{E/F^H}$$

satisfy $C \cdot \mathrm{Reg} \sim 1$ as functions to $\mathbb{R}^\times/\mathbb{Q}^{\times 2}$.

Definition 2.33. If $D < G$, we say a linear function on the Burnside ring of G is *local* (or D-*local*) if its value on any G-set only depends on the D-set structure. Since $G/H = \coprod_{x \in H\backslash G/D} D/(H^{x^{-1}} \cap D)$ as a D-set, this is equivalent to the following: there is a linear function φ_D on the Burnside ring of D such that

$$\varphi(H) = \varphi_D(\mathrm{Res}_D H) \qquad \Bigl(= \prod_{x \in H\backslash G/D} \varphi_D(H^{x^{-1}} \cap D)\ \Bigr).$$

In this case we write $\varphi = \lbrack D, \varphi_D \rbrack_G$, or simply

$$\varphi = \bigl\lbrack D, \varphi_D \bigr\rbrack.$$

Example 2.34. Such functions arise naturally in a number-theoretic setting. Suppose F/K is a Galois extension of number fields and v a place of K. Write $G = \mathrm{Gal}(F/K)$ and $D = \mathrm{Gal}(F_z/K_v)$ for the local Galois group at v (more precisely, a fixed decomposition group at v, so $D < G$). Under Galois correspondence, φ_D associates something to every extension of K_v, in which case $\varphi = \lbrack D, \varphi_D \rbrack$ simply means

$$\varphi(L) = \prod_{\text{places } w|v \text{ in } L} \varphi_D(L_w)\,.$$

(The double cosets HxD correspond to the places w of $L = F^H$ above v, and $H \cap D^x$ are their decomposition groups in $\mathrm{Gal}(F/L) = H$.) Typical local functions are those counting primes w above v in F^H, or primes with a given residue field $\mathbb{F}_q$:

$$H \mapsto \lambda^{\#\{w \text{ above } v \text{ in } F^H\}} \qquad (= \lbrack D, \lambda \rbrack)$$

$$H \mapsto \lambda^{\#\{w \text{ above } v \text{ in } F^H \text{ with } k(F^H_w) \cong \mathbb{F}_q\}} \qquad \Bigl(= \Bigl\lbrack D, H \mapsto \Bigl\{\begin{smallmatrix} \lambda, & k(F^H_w) \cong \mathbb{F}_q \\ 1, & \text{else} \end{smallmatrix}\Bigr\}\Bigr\rbrack\Bigr),$$

where $k(\cdot)$ denotes residue field. Another example is the function

$$H \mapsto \prod\nolimits_{w|v} c_w(A/F^H)\,,$$

that for an abelian variety A/K computes the product of local Tamagawa

numbers in F^H above v.

Let $I \triangleleft D$ be the inertia subgroup. If a place w of F^H corresponds to a double coset HxD, its decomposition and inertia groups in F/F^H are $H \cap D^x$ and $H \cap I^x$, respectively. Its ramification and residue degree over v are $e_w = \frac{|I|}{|H\cap I^x|}$ and $f_w = \frac{[D:I]}{[H\cap D^x : H\cap I^x]}$ (the order of Frobenius in F/K divided by that in F/F^H). Many of the local functions that we will consider in §3 can be expressed through e and f, which motivates the following definition.

Definition 2.35. Suppose $I \triangleleft D < G$ with D/I cyclic, and $\psi(e,f)$ is a function of two variables $e, f \in \mathbb{N}$. Define

$$\big(D, I, \psi\big): \quad H \longmapsto \prod_{x \in H\backslash G/D} \psi\big(\tfrac{|I|}{|H\cap I^x|}, \tfrac{[D:I]}{[H\cap D^x : H\cap I^x]}\big)\ ,$$

the product being taken over any set of representatives of the double cosets. This is a D-local function on the Burnside ring of G, to be precise

$$\big(D, I, \psi\big) = \big(D, U \mapsto \psi\big(\tfrac{|I|}{|U\cap I|}, \tfrac{|D|}{|UI|}\big)\big).$$

Theorem 2.36. *Let $I \triangleleft D < G$ with D/I cyclic. Then*

- (ℓ) *(Localisation) If $\varphi = (D, \varphi_D)$, and φ_D is trivial on D-relations, then φ is trivial on G-relations.*
- (q) *(Quotient) If $N \triangleleft G$ and $\varphi(H) = \varphi_{G/N}(HN/N)$ for some function $\varphi_{G/N}$ on the Burnside ring of G/N which is trivial on G/N-relations, then φ is trivial on G-relations.*
- (t) *(Transitivity) If $D_1 < D_2 < G$, $\varphi = (D_2, \varphi_2)_G$ and $\varphi_2 = (D_1, \varphi_1)_{D_2}$, then $\varphi = (D_1, \varphi_1)_G$.*
- (f) *(Functions of f) If $\psi(e,f)$ does not depend on e, then $(D, I, \psi) \sim 1$.*
- (r) *(Renaming) If $I_0 < I$ is normal in D with cyclic quotient, and $\psi(e,f)$ is a function of the product ef, then $(D, I, \psi) = (D, I_0, \psi)$.*
- (d) *(Descent) If $I < D_0 < D$ and $\psi(e,f) = \psi(e, f/m)^m$ whenever m divides f and $[D:D_0]$, then $(D, I, \psi) = (D_0, I, \psi)$.*

Proof. (ℓ) and (q) follow from Theorem 2.8(6) and (5), respectively. (t) is immediate from the G-set interpretation in Definition 2.33. (f) follows from properties (ℓ) and (q), and that the cyclic group D/I has no non-trivial relations. (r), (d) follow from the definitions. □

Example 2.37. Property (f) shows that the two functions $H \mapsto \lambda^{\#\cdots}$ counting primes in Example 2.34 are representation-theoretic, in other words they cancel in relations. For instance, suppose that F/K is a Galois extension of number fields and $\sum_i H_i - \sum_j H'_j$ is a $\mathrm{Gal}(F/K)$-relation. Writing $L_i = F^{H_i}$ and $L'_j = F^{H'_j}$,

$$\sum\nolimits_i \#\{\text{real places of } L_i\} = \sum\nolimits_j \#\{\text{real places of } L'_j\}\ .$$

The same is true for complex places, or primes above a fixed prime v of K with a given residue degree over v. (This does not work when counting primes with a given ramification degree instead.)

Example 2.38. If $W < G$ is a subgroup of odd order, then $(W, W, e) \sim 1$ as functions to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. For W is solvable by the Feit-Thompson theorem, and picking $W_0 \triangleleft W$ of prime index p,

$$\big(W, W, e\big) \overset{2.36\mathrm{r}}{=} \big(W, W_0, ef\big) \overset{2.36\mathrm{f}}{\sim} \big(W, W_0, e\big) \overset{2.36\mathrm{d}}{=} \big(W_0, W_0, e\big).$$

The assertion follows by induction. (The inductive step fails for $p = 2$, e.g. for $G = \mathrm{C}_2 \times \mathrm{C}_2$ the function (G, G, e) does not cancel in the relation of Example 2.3.)

Finally, we record a variant of the "descent" criterion of Theorem 2.36d.

Lemma 2.39 (Refined p-descent)**.** *Let $N \triangleleft G$ be of prime index p. Suppose ϕ, ψ are functions on the Burnside rings of G and N respectively. Then $\phi = (N, \psi)$ if and only if*

- *$\phi(H) = \psi(H \cap N)$ if $H \not\subset N$, and*
- *$\phi(H) = \prod_{x \in G/N} \psi(xHx^{-1})$ if $H \subset N$, for any choice of representatives.*

Proof. The double cosets $H \backslash G/N$ are precisely the left cosets G/N for $H \subset N$, and there is a unique double coset otherwise. □

2.iv. $\mathfrak{D}_\rho$ **and** $\mathbf{T}_{\Theta,p}$**.**
We now introduce the function $\mathfrak{D}_\rho$ that computes regulator constants, and use it to study their properties. Once again, $\mathcal{K}$ is any field of characteristic zero. At the end of the section, we reformulate these results for $\mathcal{K} = \mathbb{Q}_p$ in terms of the sets $\mathbf{T}_{\Theta,p}$ of §1.iii.

Definition 2.40. For a self-dual $\mathcal{K}G$-representation ρ with a non-degenerate $\mathcal{K}$-valued G-invariant bilinear pairing $\langle,\rangle$, define

$$\mathfrak{D}_\rho : \ H \longmapsto \det\big(\tfrac{1}{|H|}\langle,\rangle|\rho^H\big) \ \in \mathcal{K}^\times/\mathcal{K}^{\times 2}.$$

By G-invariance of the pairing, $\mathfrak{D}_\rho(H) = \mathfrak{D}_\rho(xHx^{-1})$, so this is indeed a function on the Burnside ring. If Θ is a G-relation, then by definition of regulator constants

$$\mathfrak{D}_\rho(\Theta) = \mathcal{C}_\Theta(\rho).$$

Up to $\sim$, this function is independent of the pairing: if $\mathfrak{D}'_\rho$ is defined in the same way but with a different pairing on ρ, then $\mathfrak{D}_\rho \sim \mathfrak{D}'_\rho$ by Theorem 2.17. In particular, $\mathfrak{D}_{\rho\oplus\rho'} \sim \mathfrak{D}_\rho \mathfrak{D}_{\rho'}$.

Example 2.41. $\mathfrak{D}_{\mathbf{1}}$ is the function $H \mapsto |H| \in \mathcal{K}^\times/\mathcal{K}^{\times 2}$, and $\mathfrak{D}_{\mathcal{K}[G]}$ is the constant function $H \mapsto 1$ (cf. Example 2.19).

Remark 2.42. The function $\mathfrak{D}_\rho$ is representation-theoretic (i.e. ~ 1) if and only if ρ has trivial regulator constants in all G-relations. For example, this happens if ρ carries a non-degenerate G-invariant alternating form (Theorem 2.24). On the other hand, $\mathcal{C}_\Theta(\mathbf{1})$ need not be trivial, so $\mathfrak{D}_{\mathbf{1}} \not\sim 1$ in general (cf. 2.20–2.23, 2.29).

Lemma 2.43. *If $D < G$ and ρ is a self-dual $\mathcal{K}D$-representation, then*

$$\mathfrak{D}_{\mathrm{Ind}_D^G \rho} \sim \big(D, \mathfrak{D}_\rho\big)$$

as functions to $\mathcal{K}^\times/\mathcal{K}^{\times 2}$.

Proof. Pick a D-invariant non-degenerate $\mathcal{K}$-bilinear pairing $\langle,\rangle$ on ρ. For a D-set X, define a pairing $(,)$ on $\mathrm{Hom}(X, \rho)$ by

$$(f_1, f_2) = \tfrac{1}{|D|} \sum_{x \in X} \langle f_1(x), f_2(x) \rangle, \qquad f_1, f_2 \in \mathrm{Hom}(X, \rho).$$

If $X = D/U$, the pairing $(,)$ on $\mathrm{Hom}_D(X, \rho) \subset \mathrm{Hom}(X, \rho)$ agrees with $\frac{1}{|U|}\langle,\rangle$ on $\rho^U \subset \rho$ under the identification $\mathrm{Hom}_D(D/U, \rho) = \rho^U$ given by $f \mapsto f(1)$. So for a general D-set $X = \coprod_i D/U_i$,

$$\mathfrak{D}_\rho\big(\textstyle\sum_i U_i\big) = \det\big((,) \,\big|\, \mathrm{Hom}_D(X, \rho)\big).$$

Applying this to $X = G/H$, we have

$$\begin{array}{rcl} \big(D, \mathfrak{D}_\rho\big)(H) & = & \mathfrak{D}_\rho(\mathrm{Res}_D H) = \det\big((,) \,\big|\, \mathrm{Hom}_D(G/H, \rho)\big) \\ & = & \det\big(\frac{1}{|H|}(,) \,\big|\, [\mathrm{Hom}_D(G, \rho)]^H\big) = \mathfrak{D}_{\mathrm{Ind}_D^G \rho}(H), \end{array}$$

where the last equality uses that $(,)$ is in fact a G-invariant pairing on $\mathrm{Hom}_D(G, \rho) = \mathrm{Ind}_D^G \rho$. $\square$

Corollary 2.44. *Let $I \triangleleft D < G$ with D/I cyclic. As functions to $\mathcal{K}^\times/\mathcal{K}^{\times 2}$,*

$$\mathfrak{D}_{\mathcal{K}[G/D]} \overset{2.43}{\sim} \big(D, \mathfrak{D}_{\mathbf{1}}\big) \sim \big(D, H \mapsto \tfrac{1}{|H|}\big) \overset{2.36\mathrm{f}}{\sim} \big(D, H \mapsto \tfrac{|D|}{|H|}\big) = \big(D, I, ef\big).$$

Regulator constants behave as follows under lifting, induction and restriction of relations (cf. Theorem 2.8).

Proposition 2.45. *Let ρ be a self-dual $\mathcal{K}G$-representation.*

1. *Suppose $G = \tilde{G}/N$ and Θ is a G-relation. Lifting Θ to a $\tilde{G}$-relation $\tilde{\Theta}$, we have $\mathcal{C}_{\tilde{\Theta}}(\rho) = \mathcal{C}_\Theta(\rho)$.*
2. *If $G < U$ and Θ is a U-relation, then $\mathcal{C}_\Theta(\mathrm{Ind}_G^U \rho) = \mathcal{C}_{\mathrm{Res}_G \Theta}(\rho)$.*
3. *If $D < G$ and Θ is a D-relation, then $\mathcal{C}_\Theta(\mathrm{Res}_D \rho) = \mathcal{C}_{\mathrm{Ind}_D^G \Theta}(\rho)$.*

Proof. (1) The left- and the right-hand side are the same expression up to a factor of $\prod_i |N|^{n_i \dim \rho^{H_i}}$, if we write $\Theta = \sum_i n_i H_i$. This factor equals 1 by Lemma 2.16. (2) This is a reformulation of Lemma 2.43. (3) Clear. $\square$

In view of Example 2.41, the regular representation has trivial regulator constants. Generally, we have

Lemma 2.46. *If $H < G$ is cyclic, $\mathcal{C}_\Theta(\mathcal{K}[G/H]) = 1$ for every G-relation Θ.*

Proof. For H cyclic, $\mathfrak{D}_{\mathcal{K}[G/H]} \overset{2.44}{\sim} \big(H, 1, f\big) \overset{2.36\mathrm{f}}{\sim} 1$. $\square$

Theorem 2.47. *If G has odd order, then $\mathcal{C}_\Theta(\rho) = 1$ for every G-relation Θ and every self-dual $\mathcal{K}G$-representation ρ.*

Proof. The only self-dual irreducible $\bar{\mathcal{K}}G$-representation is the trivial one. (Their number coincides with the number of self-inverse conjugacy classes of G, but these have odd order and so, except for the trivial class, have no self-inverse elements.) By Corollary 2.25(3), if ρ does not contain $\mathbf{1}$, then $\mathcal{C}_\Theta(\rho)=1$. But then $\mathcal{C}_\Theta(\mathbf{1})=\mathcal{C}_\Theta(\mathcal{K}[G])$, which is 1 by Lemma 2.46. $\square$

Corollary 2.48. *$\mathcal{C}_\Theta(\mathcal{K}[G/H])=1$ if $H<G$ has odd order.*

Proof. $\mathcal{C}_\Theta(\mathcal{K}[G/H]) \overset{2.45(2)}{=} \mathcal{C}_{\mathrm{Res}_H \Theta}(\mathbf{1}_H)=1.$ $\square$

Lemma 2.49. *Suppose $\mathcal{K}=\mathbb{Q}$ or $\mathcal{K}=\mathbb{Q}_p$, and $N \lhd H<G$ with H/N cyclic. If $p\nmid |N|$, then $\mathrm{ord}_p\, \mathcal{C}_\Theta(\mathcal{K}[G/H])$ is even for every G-relation Θ.*

Proof. $\mathfrak{D}_{\mathcal{K}[G/H]} \overset{2.44}{\sim} (H,N,ef) \overset{2.36\mathrm{f}}{\sim} (H,N,e)$ and the values of e are divisors of $|N|$. So $\mathcal{C}_\Theta(\mathcal{K}[G/H])=\mathfrak{D}_{\mathcal{K}[G/H]}(\Theta)$ has even p-valuation for $p\nmid |N|$. $\square$

Reformulation for $\mathcal{K}=\mathbb{Q}_p$. We now define the sets of representations $\mathbf{T}_{\Theta,p}$ that encode those representations whose regulator constants are "p-adicially non-trivial". It is for these twists that we prove the p-parity conjecture (Theorem 1.6). So let us also restate the properties of regulator constants in this language ($\mathbf{T}_{\Theta,p}$-ese?)

Definition 2.50. Suppose $\mathcal{K}=\mathbb{Q}_p$. For a G-relation Θ define $\mathbf{T}_{\Theta,p}$ to be the set of self-dual $\bar{\mathbb{Q}}_pG$-representations τ that satisfy

$$\langle \tau,\rho\rangle \equiv \mathrm{ord}_p\, \mathcal{C}_\Theta(\rho) \mod 2$$

for every self-dual $\mathbb{Q}_pG$-representation ρ.

Remark 2.51. For instance, $\mathbf{T}_{\Theta,p}$ contains representations of the form

$$\bigoplus_{\substack{\rho \text{ self-dual } \mathbb{Q}_p\text{-irr.}\\ \mathrm{ord}_p \mathcal{C}_\Theta(\rho) \text{ odd}}} (\text{any } \bar{\mathbb{Q}}_p\text{-irreducible constituent of } \rho).$$

These are indeed self-dual, since $\mathcal{C}_\Theta(\sigma\oplus\sigma^*)=1$ by Corollary 2.25. Note also that these particular representations have no symplectic constituents or those with even Schur index, by the same corollary.

A general element of $\mathbf{T}_{\Theta,p}$ differs from this one by something in $\mathbf{T}_{0,p}$, in other words by a self-dual (virtual) $\bar{\mathbb{Q}}_p$-representation whose inner product with any self-dual $\mathbb{Q}_p$-representation is even. Concretely, $\mathbf{T}_{0,p}$ is generated by representations of the form $\sigma\oplus\sigma^*$ (in particular $\sigma^{\oplus 2}$ for self-dual σ), and irreducible self-dual σ with either an even number of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugates or even Schur index over $\mathbb{Q}_p$.

In the context of the p-parity conjecture, the elements of $\mathbf{T}_{0,p}$ correspond to twists τ for which the conjecture should "trivially" hold. The parity of $\langle \tau, \mathcal{X}_p(A/F)\rangle$ is even, and we expect $w(A,\tau)=1$ for these τ. (This is indeed the case whenever we have an explicit formula for this root number.)

Example 2.52. If $G = \mathrm{C}_n$ is cyclic, $\Theta = 0$ is the only G-relation. The set $\mathbf{T}_{0,p}$ consists of $\mathbb{Z}$-linear combinations of $\mathbf{1}^{\oplus 2}$, $\mathrm{sign}^{\oplus 2}$ for n even, and $\chi \oplus \chi^*$ for all the remaining 1-dimensionals χ.

Example 2.53. If $G = \mathrm{D}_{2p}$ with p odd, and $\Theta = \{1\} - 2\mathrm{C}_2 - \mathrm{C}_p + 2\,G$ of Example 2.20, then $\tau \in \mathbf{T}_{\Theta,p}$ if and only if τ contains an odd number of trivial representations, an odd number of sign representations, and in total an odd number of 2-dimensional $\bar{\mathbb{Q}}_p$-irreducibles.

Example 2.54. If $G = \mathrm{D}_{2p^n}$, and τ any 2-dimensional $\bar{\mathbb{Q}}_p G$-representation, Examples 2.21, 2.22 show that $\tau \oplus \mathbf{1} \oplus \det \tau$ lies in $\mathbf{T}_{\Theta,p}$ for some G-relation Θ.

Example 2.55. If $G = \mathrm{A}_5$, its complex- (or $\bar{\mathbb{Q}}_p$-) irreducible representations are $\mathbf{1}$, 3-dimensional τ_1, τ_2, 4-dimensional χ and 5-dimensional π. Here

$$\mathbf{1} \oplus \pi \in \mathbf{T}_{\Theta,2} \qquad \mathbf{1} \oplus \chi \oplus \pi \in \mathbf{T}_{\Theta',3} \qquad \mathbf{1} \oplus \tau_i \oplus \chi \in \mathbf{T}_{\Theta'',5}\ ,$$

for some G-relations $\Theta, \Theta', \Theta''$ (see [6] Ex. 2.19).

Theorem 2.56 (Properties of $\mathbf{T}_{\Theta,p}$)**.** *Let Θ be a G-relation and $\tau \in \mathbf{T}_{\Theta,p}$.*

(1) *τ has even dimension and trivial determinant.*
(2) *$\tau \oplus \tau' \in \mathbf{T}_{\Theta+\Theta',p}$ for $\tau' \in \mathbf{T}_{\Theta',p}$.*
(3) *$\tilde{\tau} \in \mathbf{T}_{\tilde{\Theta},p}$ whenever $G = \tilde{G}/N$, and $\tilde{\tau}$, $\tilde{\Theta}$ are lifts of τ and Θ to $\tilde{G}$.*
(4) *If $D < G$, then $\mathrm{Res}_D\, \tau \in \mathbf{T}_{\mathrm{Res}_D \Theta,p}$.*
(5) *If $G < U$, then $\mathrm{Ind}_G^U\, \tau \in \mathbf{T}_{\mathrm{Ind}_G^U \Theta,p}$.*
(6) *$\langle \tau, \mathbb{Q}_p[G/H] \rangle$ is even whenever $H < G$ is cyclic, has odd order or contains a normal subgroup $N \lhd H$ with H/N cyclic and $p \nmid |N|$.*
(7) *If $|G|$ is odd or coprime to p, then $\mathbf{T}_{\Theta,p} = \mathbf{T}_{0,p}$.*

Proof. (2) Clear.
(3) Proposition 2.45(1) and Lemma 2.26.
(4) Take any self-dual $\mathbb{Q}_p D$-representation ρ. Then modulo 2,

$$\langle\, \mathrm{Res}_D\, \tau, \rho \rangle = \langle \tau, \mathrm{Ind}_D^G\, \rho \rangle \equiv \mathrm{ord}_p\, \mathcal{C}_\Theta(\mathrm{Ind}_D^G\, \rho) \overset{2.45(2)}{\equiv} \mathrm{ord}_p\, \mathcal{C}_{\mathrm{Res}_D \Theta}(\rho).$$

(5) Same computation, using Proposition 2.45(3).
(6), (7) Reformulation of 2.28 and 2.46–2.49.
(1) $\dim \tau = \langle \tau, \mathbb{Q}_p[G] \rangle$ is even by (6). Now $\det \tau(g) = 1$ for all $g \in G$ if and only if $\det \mathrm{Res}_H\, \tau = \mathbf{1}$ for all cyclic $H < G$. So (4) reduces the problem to cyclic groups, where it is clear (see Example 2.52). $\square$

Corollary 2.57. *$\mathbf{1} \notin \mathbf{T}_{\Theta,p}$ and $\mathbf{1} \oplus \epsilon \notin \mathbf{T}_{\Theta,p}$ for any 1-dimensional $\epsilon \not\cong \mathbf{1}$.*

Remark 2.58. In view of Theorems 1.14 and 1.6 we may call $\mathbf{T}_p = \bigcup_\Theta \mathbf{T}_{\Theta,p}$ the space of "p-computable" twists. This set of representations is canonically associated to a finite group G and a prime number p. It behaves well under restriction and induction, and is closed under direct sums and tensor product with permutation representations (since $\tau \otimes \mathrm{Ind}_H^G\, \mathbf{1} = \mathrm{Ind}_H^G(\mathrm{Res}_H\, \tau)$ lies in $\mathbf{T}_{\mathrm{Ind}_H^G \mathrm{Res}_H \Theta,p}$). It would be very nice to have an intrinsic description of $\mathbf{T}_p$.

3. Root numbers and Tamagawa numbers

The aim of this section is to establish the following statement about compatibility of local root numbers and local Tamagawa numbers. The proof will occupy all of §§3.i–3.v. But first, we will explain how together with Theorem 1.14 it implies Theorem 1.6, the central result of this paper on the p-parity conjecture. In fact, we expect the theorem below to hold for all principally polarised abelian varieties, and this would imply that the restrictions on the reduction of A in Theorem 1.6 could be removed.

Notation 3.1. Let K be a local field of characteristic zero, F/K a Galois extension, and A/K an abelian variety. For $H < \mathrm{Gal}(F/K)$ write (cf. §1.vi)

$$C_v(H) = C_v(A/F^H) = C_v(A/F^H, \omega^o)$$

for any exterior form ω^o on A/K, minimal if K is non-Archimedean. (We insist on minimality only for convenience: Theorem 3.2 below holds for any choice of ω because $C_v(\cdot, \omega) \sim C_v(\cdot, \omega^o)$, cf. proof of Corollary 3.4.)

Theorem 3.2 (Existence of $\mathcal{V}$)**.** *Let K be a local field of characteristic zero, F/K a Galois extension with Galois group D and A/K a principally polarised abelian variety. Assume that either*

(1) *D is cyclic,*
(2) *$A = E$ is an elliptic curve with semistable reduction,*
(3) *$A = E$ is an elliptic curve with additive reduction and K has residue characteristic $l > 3$, or*
(4) *A/K has semistable reduction.*

Then there is a $\mathbb{Q}D$-module $\mathcal{V}$ such that

(Root) $\frac{w(A,\tau)}{w(\tau)^{2\dim A}} = (-1)^{\langle \tau, \mathcal{V}\rangle}$ *for all self-dual representations τ of D, and*

(Tam) $C_v \sim \mathfrak{D}_{\mathcal{V}}$ *as functions on the Burnside ring of D. Equivalently, for every D-relation $\Theta = \sum_i n_i H_i$,*

$$\prod\nolimits_i C_v(A/F^{H_i})^{n_i} \equiv \mathcal{C}_\Theta(\mathcal{V}) \mod \mathbb{Q}^{\times 2}.$$

In the following exceptional subcase of (4) we only claim (Tam) *up to multiples of 2:*

(4ex) *A/K is semistable, K has residue characteristic 2, the wild inertia group of F/K is non-cyclic and A/K does not acquire split semistable reduction over any odd degree extension.*

In the setting of the theorem, let Θ be a D-relation and p a prime number, odd in case (4ex). For any $\tau \in \mathbf{T}_{\Theta,p}$, we obtain a chain of equalities:

$$\frac{w(A/K,\tau)}{w(\tau)^{2\dim A}} \overset{\text{(Root)}}{=} (-1)^{\langle \tau, \mathcal{V}\rangle} = (-1)^{\mathrm{ord}_p \mathcal{C}_\Theta(\mathcal{V}\otimes\mathbb{Q}_p)} \overset{\text{(Tam)}}{=} (-1)^{\mathrm{ord}_p C_v(\Theta)}$$

(note that $C_v(\Theta) \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ even for $K = \mathbb{R}, \mathbb{C}$ by property (Tam), so $\mathrm{ord}_p C_v(\Theta)$ makes sense). By the determinant formula $w(\tau)^2 = 1$, as τ is self-dual and has trivial determinant (Theorem 2.56(1), Lemma A.1). Thus,

Corollary 3.3 (Local compatibility)**.** *Suppose F/K and A/K are as in Theorem 3.2. Let Θ be a D-relation and p a prime number, odd in case* (4ex)*. Then for every $\tau \in \mathbf{T}_{\Theta,p}$,*

$$w(A/K,\tau) = (-1)^{\operatorname{ord}_p C_v(\Theta)}.$$

Now let us deduce Theorem 1.6. Suppose F/K is a Galois extension of *number fields*, A/K an abelian variety and v a place of K. Fix a non-zero regular exterior form ω on A/K, and define functions on the Burnside ring of $\mathrm{Gal}(F/K)$ by

$$C_{w|v}:\ H \mapsto \prod_{w|v} C_w(A/F^H,\omega) \qquad\qquad C:\ H \mapsto C_{A/F^H}\ \bigl(=\prod_{v} C_{w|v}(H)\bigr)\,,$$

the first product taken over the places of F^H above v.

Corollary 3.4. *Let F/K be a Galois extension of number fields, A/K an abelian variety, and fix a place z of F above a place v of K. Suppose A/K_v, F_z/K_v satisfy the assumptions of Theorem 3.2, and let p be a prime number, odd in case* (4ex)*. Then for every* $\mathrm{Gal}(F/K)$*-relation Θ and $\tau \in \mathbf{T}_{\Theta,p}$,*

$$w(A/K_v, \operatorname{Res}_{\mathrm{Gal}(F_z/K_v)} \tau) = (-1)^{\operatorname{ord}_p C_{w|v}(\Theta)}.$$

If the assumptions hold at all places v of K, then

$$w(A/K,\tau) = (-1)^{\operatorname{ord}_p C(\Theta)}.$$

Proof. Write $D = \mathrm{Gal}(F_z/K_v) < \mathrm{Gal}(F/K)$ for the decomposition group of z, and I for its inertia subgroup. First note that $C_{w|v}(\Theta)$ is independent of the choice of the exterior form ω: if $\omega = \alpha\omega'$, then

$$\frac{\prod_{w|v} C_w(A/F^H,\omega)}{\prod_{w|v} C_w(A/F^H,\omega')} = \prod_{w|v} |\alpha|_{F^H_w} = \bigl(D, I, |\alpha|^f_{K_v}\bigr)(H)\,,$$

and this function is trivial on Θ by Theorem 2.36f. So we may assume that ω is minimal at v.

Now $\operatorname{Res}_D \tau \in \mathbf{T}_{\operatorname{Res}_D \Theta,p}$ by Theorem 2.56(4), so

$$\begin{aligned} w(A/K_v, \operatorname{Res}_D \tau) &= (-1)^{\operatorname{ord}_p C_v(\operatorname{Res}_D \Theta)} && \text{(Corollary 3.3)}\\ &= (-1)^{\operatorname{ord}_p C_{w|v}(\Theta)} && \text{(as } C_{w|v} = (D, C_v)\text{, cf. 2.33, 2.34).} \end{aligned}$$

For the last claim, take the product over all places. ∎

Proof of Theorem 1.6. The abelian variety A/K satisfies the hypothesis of Corollary 3.4 at all places of K. So for every $\tau \in \mathbf{T}_{\Theta,p}$

$$w(A/K,\tau) \overset{3.4}{=} (-1)^{\operatorname{ord}_p C(\Theta)} \overset{1.14}{=} (-1)^{\langle \tau, \mathcal{X}_p(A/F)\rangle}.$$

∎

3.i. **Setup.** In the remainder of §3 we prove Theorem 3.2. Let A/K and F/K be as in the theorem, in particular K is again *local*. We split cases (1)-(3) into subcases and define an extension L of K as follows:

Notation 3.5.

(1) D is cyclic.
 - (1-) $|D|$ is odd; $L = K$.
 - (1+) $|D|$ is even; L is the unique quadratic extension of K inside F.

(2) $A = E$ is an elliptic curve with semistable reduction.
 - (2G) E has good reduction; $L = K$.
 - (2S) E has split multiplicative reduction; $L = K$.
 - (2NS) E has non-split multiplicative reduction; L/K is quadratic unramified.

(3) $A = E$ is an elliptic curve with additive reduction, K has residue characteristic $l > 3$. Write Δ_E and c_6 for the standard invariants of some model of E/K and $\mathfrak{e} = \frac{12}{\gcd(12, \operatorname{ord}\Delta_E)}$.
 - (3C) E has potentially good reduction, $\mu_{\mathfrak{e}} \subset K$; $L = K(\sqrt[\mathfrak{e}]{\Delta_E})$, a cyclic extension of K.
 - (3D) E has potentially good reduction, $\mu_{\mathfrak{e}} \not\subset K$; $L = K(\mu_{\mathfrak{e}}, \sqrt[\mathfrak{e}]{\Delta_E})$, a dihedral extension of K.
 - (3M) E has potentially multiplicative reduction; $L = K(\sqrt{-c_6})$.

(4) A/K has semistable reduction; L is the smallest unramified extension of K where A acquires split semistable reduction.

We remind the reader that (4) has a subcase (4ex), see Theorem 3.2. Note that (1) includes Archimedean places, and in (2)-(4) L is a minimal Galois extension of K where A acquires split semistable reduction (cf. Lemma 3.22).

In view of Lemma 3.8 below, we may and will henceforth assume

Hypothesis 3.6. *F contains L.*

Notation 3.7. Henceforth write

$$\begin{array}{lcl} D & = & \mathrm{Gal}(F/K), \\ D' & = & \mathrm{Gal}(F/L) \triangleleft D, \\ I & = & \text{Inertia subgroup of } D, \\ W & = & \text{Wild inertia subgroup of } I. \end{array}$$

We work extensively with functions from the Burnside ring of D to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. For brevity, $(\cdots)$ stands for $(\cdots)_D$ in §§3.ii–3.v (see Definitions 2.33, 2.35).

Lemma 3.8. *Suppose $\mathcal{V}$ is a $\mathbb{Q}G$-module and M/K a Galois extension contained in F. If $\mathcal{V}$ satisfies* (Root) *and the p-part of* (Tam) *of Theorem 3.2, then $\mathcal{W} = \mathcal{V}^{\mathrm{Gal}(F/M)}$ satisfies the same conditions for the extension M/K.*

Proof. The irreducible constituents of $\mathcal{W}$ are precisely those of $\mathcal{V}$ that factor through $\mathrm{Gal}(M/K)$, so $\mathcal{W}$ clearly satisfies (Root). If Θ is a $\mathrm{Gal}(M/K)$-relation and $\tilde{\Theta}$ is its lift to G (as in Theorem 2.8(3)), then $\mathcal{C}_{\tilde{\Theta}}(\mathcal{V} \ominus \mathcal{W}) = 1$ by Lemma 2.26. So $\mathcal{W}$ satisfies (Tam). □

The choice of $\mathcal{V}$ is forced by formulae for the local root numbers $w(A/K,\tau)$. For a self-dual representation τ of $\mathrm{Gal}(F/K)$, we claim that

$$w(A/K,\tau) = w(\tau)^{2\dim A}\,\lambda^{\dim\tau}\,(-1)^{\langle\tau,V\rangle}$$

with $\lambda=\pm1$ and the representation V of D/D' given in Table 3.9. Here

Case	D/D'	λ	V
(1-)	1	$w(A/K)$	0
(1+)	C_2	$w(A/K)$	$\chi^{\oplus b}$
(2G)	1	1	0
(2S)	1	1	$\mathbf{1}$
(2NS)	C_2	1	η
(3C)	$\mathrm{C}_2,\mathrm{C}_3,\mathrm{C}_4,\mathrm{C}_6$	ϵ	0
(3D)	$\mathrm{D}_6,\mathrm{D}_8,\mathrm{D}_{12}$	$-\epsilon$	$\mathbf{1}\oplus\eta\oplus\sigma$
(3M)	C_2	$w(\chi)^2$	χ
(4)	cyclic	1	$X(\mathcal{T}^*)\otimes\mathbb{Q}$

Table 3.9. Root numbers

$\mathbf{1},\chi,\eta$ and σ are the trivial character, the non-trivial character of order 2, the unramified quadratic character and the unique faithful 2-dimensional representation of D/D'. The exponent b is defined by $(-1)^b=\frac{w(A/K,\mathbf{1}\oplus\chi)}{w(\chi)^{2\dim A}}$, ϵ is as in [30] Thm. 2 (we will not need it explicitly) and $X(\mathcal{T}^*)$ is the character group of the torus in the Raynaud parametrisation of the dual abelian variety A^t, see §3.v.

Granting the claim, define

$$\mathcal{V} = V \;\;\oplus\;\; \begin{cases} 0, & \lambda=1,\\ \mathbb{Q}[D], & \lambda=-1.\end{cases}$$

By Frobenius reciprocity, $\langle\tau,\mathbb{Q}[D]\rangle=\dim\tau$, so $\mathcal{V}$ satisfies property (Root) of Theorem 3.2. Moreover, $\mathfrak{D}_{\mathbb{Q}[D]}\sim 1$ by Lemma 2.46, so $\mathfrak{D}_{\mathcal{V}}\sim\mathfrak{D}_V$.

It remains to prove the following

Proposition 3.10. *In each of the cases (1)–(4) and V,λ as in Table 3.9, we have $\mathfrak{D}_V\sim C_v$ (up to multiples of 2 in case* (4ex)*) and*

$$w(A/K,\tau) = w(\tau)^{2\dim A}\,\lambda^{\dim\tau}\,(-1)^{\langle\tau,V\rangle}$$

for every self-dual representation τ of $\mathrm{Gal}(F/K)$.

The proof is a case-by-case analysis and will occupy §3.ii–§3.v.

3.ii. Case (1): Cyclic decomposition group.

Lemma 3.11. *Suppose $D=\mathrm{Gal}(F/K)$ is cyclic. Then*

$$w(A/K,\tau)=w(\tau)^{2\dim A}w(A/K)^{\dim\tau} \qquad \textit{if}\quad 2\nmid[F:K],$$
$$w(A/K,\tau)=w(\tau)^{2\dim A}w(A/K)^{\dim\tau}\Big(\frac{w(A/K,\mathbf{1}\oplus\chi)}{w(\chi)^{2\dim A}}\Big)^{\langle\tau,\chi\rangle} \qquad \textit{if}\quad 2\,|\,[F:K].$$

Moreover, $w(A/K)$ and $\frac{w(A/K,\mathbf{1}\oplus\chi)}{w(\chi)^{2\dim A}}$ are ±1.

Proof. For the last claim, local root numbers of abelian varieties are ± 1, see e.g. [34] §1.1. So $w(A/K) = \pm 1$, and the same holds for the quadratic twist of A by χ. By the determinant formula, $w(\chi)^2 = \pm 1$ as well (Lemma A.1).

By Lemma A.1, $w(A/K, \rho \oplus \rho^*) = 1$ for every representation ρ, so it suffices to check the formulae for $\tau = \mathbf{1}$ and for $\tau = \chi$ when $[F : K]$ is even. But this is clear as $w(\mathbf{1}) = 1$. $\square$

As D is cyclic and has therefore no relations, we trivially have $C_v \sim 1 \sim \mathfrak{D}_V$. This proves Proposition 3.10 in Case (1).

3.iii. **Case (2): Semistable elliptic curves.** The root number formula follows from [30] Thm. 2 and the determinant formula (Lemma A.1).

We now prove that $\mathfrak{D}_V \sim C_v$. Note that the differential ω remains minimal in all extensions of K, so $C_v(E/F^H) = c_v(E/F^H)$ for all $H < D$. By Tate's algorithm ([38], IV.9), in terms of $e = e_{F^H/K}$ and $f = f_{F^H/K}$ these Tamagawa numbers are:

Reduction of E/K	Good	Split I_n	Non-split I_n
$c_v(E/F^H)$	1	ne	$\begin{cases} 1, & 2\nmid f, 2\nmid ne, \\ 2, & 2\nmid f, 2\mid ne, \\ ne, & 2\mid f. \end{cases}$

3.iii.1. *(Case 2G) E has good reduction.* $\mathfrak{D}_V = C_v = 1$.

3.iii.2. *(Case 2S) E has split multiplicative reduction.* If E/K has type I_n,

$$\mathfrak{D}_V = \mathfrak{D}_{\mathbb{Q}[D/D]} \overset{2.44}{\sim} \big(D, I, ef\big) \overset{2.36\mathrm{f}}{\sim} \big(D, I, ne\big) = C_v.$$

3.iii.3. *(Case 2NS) E has nonsplit multiplicative reduction.* If E/K has type I_n, then

$$\begin{aligned} \mathfrak{D}_V = \mathfrak{D}_\eta \sim \mathfrak{D}_{\mathbb{Q}[D/D']}/\mathfrak{D}_{\mathbb{Q}[D/D]} &\overset{2.44}{\sim} \big(D', I, ef\big)/\big(D, I, ef\big) \\ &\overset{2.39}{=} \Big(D, I, \Big\{\begin{smallmatrix} ef, & 2\nmid f \\ (ef/2)^2, & 2|f \end{smallmatrix}\Big\}\Big)/\big(D, I, ef\big) = \Big(D, I, \Big\{\begin{smallmatrix} 1, & 2\nmid f \\ ef, & 2|f \end{smallmatrix}\Big\}\Big) \\ &\overset{2.36\mathrm{f}}{\sim} \Big(D, I, \Big\{\begin{smallmatrix} 1, & 2\nmid f \\ en, & 2|f \end{smallmatrix}\Big\}\Big) = C_v \cdot \Big(D, I, \Big\{\begin{smallmatrix} 2, & 2\nmid f, 2|ne \\ 1, & \text{else} \end{smallmatrix}\Big\}\Big). \end{aligned}$$

It remains to show that the last factor is ~ 1. If n is even, it is a function of f and therefore ~ 1 by Theorem 2.36f.

Now suppose n is odd. Then

$$\Big(D, I, \Big\{\begin{smallmatrix} 2, & 2\nmid f, 2|e \\ 1, & \text{else} \end{smallmatrix}\Big\}\Big) \overset{2.36\mathrm{d}}{=} \Big(I, I, \Big\{\begin{smallmatrix} 2, & 2|e \\ 1, & 2\nmid e \end{smallmatrix}\Big\}\Big) \overset{2.36\mathrm{r}}{=} \Big(I, W, \Big\{\begin{smallmatrix} 2, & 2|ef \\ 1, & 2\nmid ef \end{smallmatrix}\Big\}\Big).$$

If $v \nmid 2$, then W has odd order, so this is a function of f, hence ~ 1 again. Henceforth assume $v|2$, so W is a 2-group and $[I : W]$ is odd. Then

$$\Big(I, W, \Big\{\begin{smallmatrix} 2, & 2|ef \\ 1, & 2\nmid ef \end{smallmatrix}\Big\}\Big) \overset{2.36\mathrm{d}}{=} \Big(W, W, \Big\{\begin{smallmatrix} 2, & 2|e \\ 1, & 2\nmid e \end{smallmatrix}\Big\}\Big) \overset{2.36\mathrm{f}}{\sim} \Big(W, W, \Big\{\begin{smallmatrix} 1, & 2|e \\ 2, & 2\nmid e \end{smallmatrix}\Big\}\Big).$$

By Theorem 2.36ℓ, it suffices to prove that the function on subgroups of W

$$\varphi_W : H \longmapsto \Big\{\begin{smallmatrix} 1, & H \neq W \\ 2, & H = W \end{smallmatrix}\Big\}$$

is trivial on W-relations.

Let $W/\Phi = \bar{W}$ be the maximal exponent 2 quotient of W (so $\Phi \triangleleft W$ is its Frattini subgroup.) Since proper subgroups of W cannot have full image in $\bar{W}$, we have $\varphi_W(H) = \varphi_{\bar{W}}(\bar{H})$. By Theorem 2.36q, it is enough to verify that $\varphi_{\bar{W}}$ is trivial on $\bar{W}$-relations. But every $\bar{W}$-relation has an even number of terms with $H = \bar{W}$ (only these have $\mathbb{C}[\bar{W}/H]$ of odd dimension), so this is clear.

3.iv. **Case (3): Elliptic curves with additive reduction.** We now come to the truly painful case of additive reduction. Thus $l \neq 2, 3$ is a fixed prime, K a finite extension of $\mathbb{Q}_l$ and E/K has additive reduction. We write q for the size of the residue field of K and δ for the valuation of the minimal discriminant of E/K. The asserted root number formula again comes from [30] Thm. 2, and it remains to show $\mathfrak{D}_V \sim C_v$.

Decompose the functions

$$\mathfrak{D}_V = a \cdot d, \quad C_v = c_v \cdot \omega$$

with

$$\begin{array}{rclcrcl} a(H) & = & \det(\langle,\rangle|V^H) & \qquad & d(H) & = & |H|^{-\dim V^H} \\ c_v(H) & = & c_v(E/F^H) & & \omega(H) & = & \left|\frac{\omega^o_{E/K}}{\omega^o_{E/F^H}}\right|_{F^H}. \end{array}$$

These are well-defined on conjugacy classes of subgroups of D and take values in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. The pairing $\langle,\rangle$ on V may be chosen arbitrarily, and we picked one that seemed natural to give explicit values of a in Tables 3.14, 3.17 (write V as a sum of permutation modules and use Example 2.19).

The function ω may be expressed in terms of $e = e_{F^H/K}$ and $f = f_{F^H/K}$ as follows. The minimal discriminant of E/K has valuation δe over F^H, so $\omega(H) = q^{\lfloor(\delta e - \delta_H)/12\rfloor f}$ where δ_H is the valuation of the minimal discriminant of E/F^H (cf. [37] Table III.1.2). If E has potentially good reduction, then $0 \leq \delta_H < 12$. If the reduction is potentially multiplicative of type I_n^* (so $\delta = 6 + n$), it becomes I_{ne}^* over F^H if e is odd ($\delta_H = 6 + ne$), and I_{ne} if e is even ($\delta_H = ne$). It follows easily that

$$\omega = \begin{cases} (D, I, q^{\lfloor \frac{\delta e}{12} \rfloor f}), & \text{if } E \text{ has potentially good reduction} \\ (D, I, q^{\lfloor \frac{e}{2} \rfloor f}), & \text{if } E \text{ has potentially multiplicative reduction.} \end{cases}$$

3.iv.1. *Reduction to 2-power residue degree.*

Lemma 3.12. *If K''/K' is a subextension of F/K, and is unramified of odd degree, then $C_v(E/K'') \equiv C_v(E/K') \mod \mathbb{Q}^{\times 2}$.*

Proof. For c_v this follows from Lemma 3.22. For ω this is clear. □

Lemma 3.13. *It suffices to prove Case (3) of Proposition 3.10 when $f_{F/K}$ is a power of 2.*

Proof. Let $N \triangleleft D$ correspond to the maximal odd degree unramified extension of K in F. As C_v is unchanged in odd degree unramified extensions (Lemma 3.12), a repeated application of Lemma 2.39 with $\phi = \psi = C_v$

shows that $C_v = (N, C_v)$. We claim that $\mathfrak{D}_V \sim (N, \mathfrak{D}_{\mathrm{Res}_N V})$. Then, by Theorem 2.36$\ell$, it suffices to show that $\mathfrak{D}_{\mathrm{Res}_N V} \sim C_v$ as functions on the Burnside ring of N, as asserted.

By Lemma 2.43, $(N, \mathfrak{D}_{\mathrm{Res}_N V}) \sim \mathfrak{D}_{\mathrm{Ind}_N^G \mathrm{Res}_N V}$. But

$$\mathrm{Ind}_N^G \mathrm{Res}_N V \;\cong\; V \otimes \mathrm{Ind}_N^G \mathbf{1}_N \;\cong\; V \oplus J$$

with J of the form $\mathcal{J} \oplus \mathcal{J}^*$ over $\bar{\mathbb{Q}}$. By Corollary 2.25, $\mathfrak{D}_J(\Theta) = \mathcal{C}_\Theta(J) = 1$ for any D-relation Θ. Thus $\mathfrak{D}_J \sim 1$, whence $\mathfrak{D}_{\mathrm{Ind}_N^G \mathrm{Res}_N V} \sim \mathfrak{D}_V$, as required. $\square$

3.iv.2. *(Cases 3C, 3D) E/K has potentially good reduction.* By Lemma 3.13, it suffices to prove the following

Claim. Suppose $f_{F/K}$ is a power of 2. Then $c_v \sim a$ and $\omega \sim d$, and hence $C_v \sim \mathfrak{D}_V$.

Let $\mathfrak{e} = e_{L/K}$ be the ramification degree of L over K. The extension is either cyclic or dihedral (cf. Table 3.9), to be precise

$$\begin{array}{lll} \text{(Case 3C)} & \mathrm{Gal}(L/K) \cong \mathrm{C}_{\mathfrak{e}} & \mathfrak{e} = 2, 3, 4, 6, \\ \text{(Case 3D)} & \mathrm{Gal}(L/K) \cong \mathrm{D}_{2\mathfrak{e}} & \mathfrak{e} = 3, 4, 6. \end{array}$$

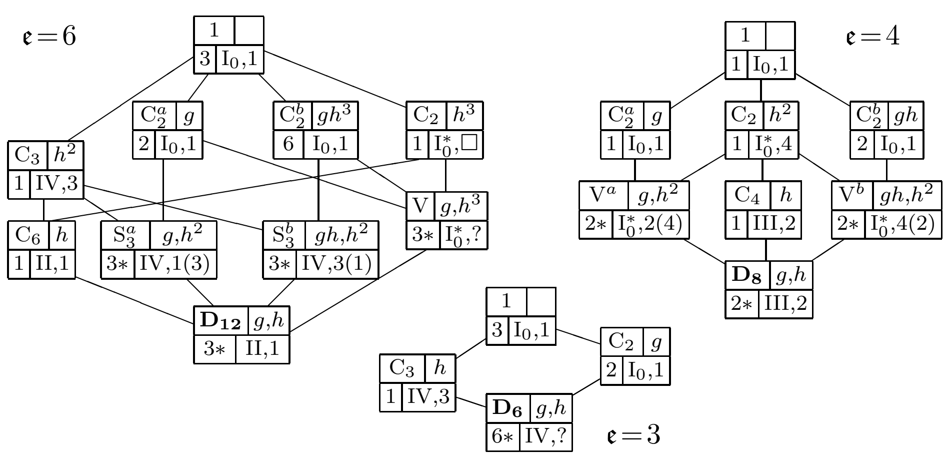
As E/L has good reduction, $\delta\mathfrak{e} \equiv 0 \mod 12$, and $\mathfrak{e}$ is the smallest such integer. Moreover, $q \equiv (-1)^t \mod \mathfrak{e}$ with $t = 0$ in Case 3C and $t = 1$ in Case 3D (see e.g. [30] Thm. 2).

As V is a $\mathrm{Gal}(L/K)$-representation, both $a(H)$ and the exponent $\dim V^H$ in $d(H)$ depend only on $F^H \cap L$. In Case 3C, $V = 0$ and $a(H) = d(H) = 1$. For Case 3D, we summarise in Table 3.14 the subgroups H (up to conjugacy) of

$$\mathrm{Gal}(L/K) = D/D' = \mathrm{D}_{2\mathfrak{e}} = \langle g, h | h^{\mathfrak{e}} = g^2 = (gh)^2 = 1 \rangle$$

with the following data: in the top row is H and its generators; in the

Table 3.14. Dihedral quotient



bottom left corner $a(H)$, followed by $*$ when $\dim V^H$ is odd; in the bottom right corner the Kodaira symbol and c_v for E/L^H. The functions a and d

are elementary to compute, and c_v come from Lemma 3.22; $\square$ denotes a square value, ? an undetermined value, $\mathrm{V}=\mathrm{C}_2\times\mathrm{C}_2$. The entries 1(3) and 3(1) for the Tamagawa numbers in the table for $\mathfrak{e}=6$ mean that there are actually two tables, one with 1 and 3 and one with 3 and 1. (Similarly for 2(4) and 4(2) when $\mathfrak{e}=4$.) There are also identical tables, but with II, III, IV replaced everywhere by II*, III* and IV*, respectively.

Remark 3.15. Note from the pictures that $c_v \sim a$ in $\mathrm{Gal}(L/K)$-relations in Case D; see Example 2.4 for the list of relations. This is also true in Case C, as $\mathrm{Gal}(L/K)$ is cyclic and has no relations. Now, a is a function lifted from $\mathrm{Gal}(L/K)$. If c_v were such a function as well, we would have $c_v \sim a$ in general by Theorem 2.36q. Unfortunately, life is not that simple, and we will use the full force of the machinery in §2 to establish the result.

Proposition 3.16. *$c_v \sim a$.*

Proof. We proceed as follows

`Step 1:  Reduction to` $D=\mathrm{C}_{\mathfrak{e}}\rtimes\mathrm{C}_{2^k}$.

We claim that a and c_v are both lifted from $\mathrm{Gal}(L^u/K)$, where we use ^{u} to denote the maximal unramified extension in F. Then by Theorem 2.36q we may replace F by L^u, and we will be left with the case $e_{F/K}=\mathfrak{e}$ and $D=\mathrm{C}_{\mathfrak{e}}\rtimes\mathrm{C}_{2^k}$.

That a lifts from $\mathrm{Gal}(L^u/K)$ is clear. In view of Lemma 3.22, to see that c_v has this property it is enough to check that for every intermediate field M of F/K, the extension $M/M\cap L^u$ is totally ramified with $\gcd(e_{M/K},\mathfrak{e})=\gcd(e_{M\cap L^u/K},\mathfrak{e})$. By Lemma 3.24, there is a subfield $K\subset M_{\mathfrak{e}}\subset M$ with $M/M_{\mathfrak{e}}$ totally ramified and $e_{M_{\mathfrak{e}}/K}=\gcd(e_{M/K},\mathfrak{e})$; so it suffices to show that $L^u\cap M$ contains $M_{\mathfrak{e}}$, equivalently that $M_{\mathfrak{e}}\subset L^u$. But $M_{\mathfrak{e}}^u/K^u$ and L^u/K^u sit inside the (cyclic) maximal tame extension F^W/K^u, so $M_{\mathfrak{e}}^u\subset L^u$ by comparison of degrees.

We now have

$$D \;=\; \mathrm{C}_{\mathfrak{e}}\rtimes\mathrm{C}_{2^k} \;=\; \langle x,y\mid x^{\mathfrak{e}}=y^{2^k}=1, yxy^{-1}=x^{\pm1}\rangle$$

with x^{+1} in Case 3C and x^{-1} in Case 3D, $I=\mathrm{C}_{\mathfrak{e}}=\langle x\rangle$ and $\mathfrak{e}=2,3,4,6$.

`Step 2:  Proof for` $\mathfrak{e}=2,3,6$.

Suppose $\mathfrak{e}=2,3$ or 6.

By Examples 2.10, 2.11 (note that $4\nmid\mathfrak{e}$), it is enough to prove that c_v/a is trivial on relations of all the subquotients H_t/N_t where

$$H_t=\langle x,y^{2^t}\rangle,\qquad N_t=\langle y^{2^{t+1}}\rangle.$$

In Case 3D, the $t=0$ quotient is $D/D'\cong\mathrm{D}_{2\mathfrak{e}}$, where c_v/a does cancel in relations by Remark 3.15. We consider the remaining subquotients ($\cong\mathrm{C}_{\mathfrak{e}}\times\mathrm{C}_2$) in Cases C and D, according to the value of $\mathfrak{e}$. If $\mathfrak{e}=3$, these are cyclic and have no relations, so the result is trivial. If $\mathfrak{e}=6$, H_t/N_t has the following lattice of subgroups. Here we specify the group name, its generators (h is the image of x, and g a suitable element of order 2), the value of a ($X=1$ in

Case 3C, and $X=3$ in Case 3D), the reduction type and Tamagawa numbers over the corresponding fields:

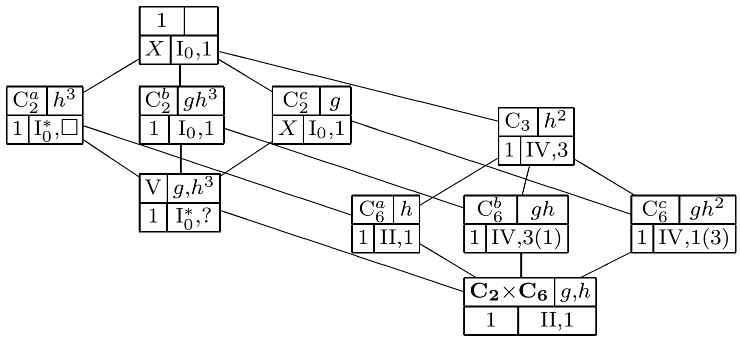


TABLE 3.17. $C_6\times C_2$ - subquotient

The lattice of relations is generated by $C_3 - C_6^a - C_6^b - C_6^c + 2(C_6\times C_2)$ and $1-C_2^a-C_2^b-C_2^c+2V$, on each of which a/c_v is trivial by inspection. Finally if $\mathfrak{e}=2$, the subquotients are isomorphic to $C_2\times C_2$, and the data for their subgroups is the same as for the subgroups of $V\subset C_6\times C_2$ in Table 3.17 with $X=1$. Once again, a/c_v is trivial on the unique $C_2\times C_2$ relation, which completes the proof that $c_v\sim a$ for $\mathfrak{e}\neq 4$.

`Step 3: Proof for` $\mathfrak{e}=4$.

Suppose $\mathfrak{e}=4$ and we are in Case 3D. By Example 2.11 and the proof of Lemma 2.9(1), every D-relation is a sum of one lifted from $D/D'\cong D_8$ and a D-relation with terms in $U=\langle x,y^2\rangle$. By Remark 3.15, c_v/a cancels in relations of D/D', so it suffices to prove cancellation in D-relations whose terms lie in U. Subgroups of U project to subgroups of C_4 in D/D', so $a=1$ for these (see Table 3.14). Hence it is enough to show that the following function cancels in D-relations with terms in U:

$$\tilde{c}_v(H)=c_v(E/F^H)\cdot\begin{cases}|H|^2, & H\subset\langle y\rangle,\\ 4, & \langle x^2\rangle\subset H\subset\langle x^2,y\rangle,\\ 1, & \text{otherwise.}\end{cases}$$

As $\langle x^2\rangle$, $\langle y\rangle$ and $\langle x^2,y\rangle$ are normal in D, the "correction terms" are the same for conjugate subgroups, so this is a function on the Burnside ring of D. Exceptionally, we view $\tilde{c}_v$ as a function to $\mathbb{R}_{>0}$, *not* (!) to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. The point is that now it suffices to check that it cancels in U-relations, since a multiple of a D-relation with terms in U is an U-relation by Lemma 2.9(1), and taking roots is perfectly ok in $\mathbb{R}_{>0}$.

By Example 2.10, U-relations are generated by those coming from the subquotients H_t/N_t $(1\leq t\leq k-2)$ with

$$H_t=\langle x,y^{2^t}\rangle,\qquad N_t=\langle y^{2^{t+2}}\rangle,\qquad H_t/N_t\;\cong\;C_4\times C_4\,.$$

In such a subquotient, let g and h be the images of x and y^{2^t} respectively. Note that the field $F^{H_t}(\sqrt{\Delta_E})$ corresponds to $\langle g^2,h\rangle$. (By Lemma 3.22, it distinguishes between $c_v=2$ and $c_v=4$ in the I_0^*-case; $c_v=1$ cannot occur

because E/K has $c_v = 2$ and so has non-trivial 2-torsion in every extension of K, see Remark 3.23.) The subquotient H_t/N_t has a basis of 5 relations, given below with the corresponding $\tilde{c}_v$:

$$\begin{array}{lcl}
\langle g^2\rangle - \langle gh^2\rangle - \langle h^2, g^2\rangle - \langle g\rangle + 2\langle g, h^2\rangle & \to & 4^1 2^{-1} 4^{-1} 2^{-1} 2^2 = 1 \\
\langle h^2, g^2\rangle - \langle g^2, h\rangle - \langle g^2, gh\rangle - \langle g, h^2\rangle + 2\langle g, h\rangle & \to & 4^1 4^{-1} 2^{-1} 2^{-1} 2^2 = 1 \\
\langle h^2 g^2\rangle - \langle g^3 h\rangle - \langle h^2, g^2\rangle - \langle gh\rangle + 2\langle g^2, gh\rangle & \to & 1^1 1^{-1} 4^{-1} 1^{-1} 2^2 = 1 \\
\{1\} - \langle g^2\rangle - \langle h^2 g^2\rangle - \langle h^2\rangle + 2\langle h^2, g^2\rangle & \to & (4^{k\text{-}t\text{-}2})^1 4^{-1} 1^{-1} (4^{k\text{-}t\text{-}1})^{-1} 4^2 = 1 \\
\langle h^2\rangle - \langle h^2, g^2\rangle - \langle h\rangle - \langle g^2 h\rangle + 2\langle g^2, h\rangle & \to & (4^{k\text{-}t\text{-}1})^1 4^{-1} (4^{k\text{-}t})^{-1} 1^{-1} 4^2 = 1.
\end{array}$$

As the $\tilde{c}_v$ cancel in all relations, this proves the claim in Case 3D.

Finally, in Case 3C the a and the c_v are the same as for the subgroup H_1 of Case 3D, so they again cancel in relations. □

Proposition 3.18. *In Case 3C, $\omega \sim 1$. In Case 3D, $\omega \sim \big(I, W, \{\begin{smallmatrix} e, & \mathfrak{e}\nmid f \\ 1, & \mathfrak{e}|f \end{smallmatrix}\}\big)$.*

Proof. As before, write δ for the valuation of the minimal discriminant of E/K and q for the size of the residue field of K. So $q \equiv (-1)^t \mod \mathfrak{e}$ with $t = 0$ in Case 3C and $t = 1$ in Case 3D. If q is an even power of the residue characteristic l, then $t = 0$ and $\omega = q^{\cdots} = 1 \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ as asserted. Suppose from now on that q is an odd power of l, so

$$\omega = \big(D, I, q^{\lfloor \frac{\delta e}{12} \rfloor f}\big) = \big(D, I, l^{\lfloor \frac{\delta e}{12} \rfloor f}\big) \overset{2.36\text{d}}{=} \big(I, I, l^{\lfloor \frac{\delta e}{12} \rfloor}\big) \overset{2.36\text{r}}{=} \big(I, W, l^{\lfloor \frac{\delta e f}{12} \rfloor}\big).$$

The order of W is a power of l, so let us define k by $e = l^k$.

Define $n \in \{0, 1\}$ by

$$l\delta \equiv q\delta \equiv (-1)^t \delta + 12n \mod 24,$$

so

$$l^k \delta \equiv (-1)^{tk} \delta + 12nk \mod 24.$$

Then

$$\omega = \big(I, W, l^{\lfloor \frac{\delta l^k f}{12} \rfloor}\big) = \big(I, W, l^{\lfloor \frac{(-1)^{tk}\delta f}{12} + fkn \rfloor}\big) = \big(I, W, l^{\lfloor \frac{(-1)^{tk}\delta f}{12} \rfloor}\big)\big(I, W, e^{fn}\big).$$

The second term is trivial:

$$\big(I, W, e^{fn}\big) \overset{2.36\text{d}}{=} \big(W, W, e^n\big) \overset{2.38}{\sim} 1.$$

As for the first term, for $t = 0$ it is a function of f so it is ~ 1 by Theorem 2.36f, as required. Finally, $\lfloor \frac{m}{12} \rfloor \equiv \lfloor \frac{-m}{12} \rfloor \mod 2$ if and only if $12|m$, so for $t = 1$ we have

$$\big(I, W, l^{\lfloor \frac{(-1)^k \delta f}{12} \rfloor}\big) = \big(I, W, l^{\lfloor \frac{\delta f}{12} \rfloor}\big)\Big(I, W, \Big\{ \begin{smallmatrix} 1, & 2|k \\ 1, & 12|\delta f \\ l, & \text{else} \end{smallmatrix} \Big\}\Big) \overset{2.36\text{f}}{\sim} \Big(I, W, \Big\{ \begin{smallmatrix} 1, & 2|k \\ 1, & 12|\delta f \\ l, & \text{else} \end{smallmatrix} \Big\}\Big)$$

$$= \Big(I, W, \Big\{ \begin{smallmatrix} l^k, & 2|k \\ 1, & \mathfrak{e}|f \\ l^k, & \text{else} \end{smallmatrix} \Big\}\Big) = \big(I, W, \{\begin{smallmatrix} e, & \mathfrak{e}\nmid f \\ 1, & \mathfrak{e}|f \end{smallmatrix}\}\big),$$

as asserted. □

Proposition 3.19. *In Case 3C, $d \sim 1$. In Case 3D, $d \sim \big(I, W, \{\begin{smallmatrix} e, & \mathfrak{e}\nmid f \\ 1, & \mathfrak{e}|f \end{smallmatrix}\}\big)$.*

Proof. In Case 3C, the module V is zero and the result is trivial, so suppose we are in Case 3D. By definition, $d(H)$ is either 1 or $|H|$ (up to squares), depending on the intersection of F^H with the dihedral extension L/K. We

may replace $|H|$ by $[D:H]=e_{F^H/K}f_{F^H/K}$ by Lemma 2.16. Inspecting $*$ in Table 3.14, we find that for $H\supset D'$ (i.e. corresponding to subfields of L),

$$(ef)^{\dim V^H}\equiv\left\{\begin{array}{ll}1, & 2|f \text{ or } \mathfrak{e}|e\\ ef, & \text{else}\end{array}\right. \mod \mathbb{Q}^{\times 2}\qquad (\text{with } e{=}e_{F^H/K},\ f{=}f_{F^H/K}).$$

By Lemmas 3.24, 3.25, the condition "$2|f$ or $\mathfrak{e}|e$" holds for a general F^H if and only if it holds for $F^H\cap L$. Therefore

$$d\ \sim\ (H\mapsto(e_{F^H/K}f_{F^H/K})^{\dim V^H})\ =\ \Bigl(D,I,\left\{\begin{smallmatrix}1, & 2|f\\ 1, & \mathfrak{e}|e\\ ef, & \text{else}\end{smallmatrix}\right\}\Bigr).$$

Recall that $2,3\nmid|W|$ and that $[D:I]$ is a power of 2 (Lemma 3.13). Thus

$$\Bigl(D,I,\left\{\begin{smallmatrix}1, & f\neq1\\ 1, & \mathfrak{e}|e\\ e, & \text{else}\end{smallmatrix}\right\}\Bigr)\overset{2.36\text{d}}{=}\Bigl(I,I,\left\{\begin{smallmatrix}1, & \mathfrak{e}|e\\ e, & \mathfrak{e}\nmid e\end{smallmatrix}\right\}\Bigr)$$
$$\overset{2.36\text{r}}{=}\Bigl(I,W,\left\{\begin{smallmatrix}1, & \mathfrak{e}|f\\ ef, & \mathfrak{e}\nmid f\end{smallmatrix}\right\}\Bigr)\overset{2.36\text{f}}{\sim}\Bigl(I,W,\left\{\begin{smallmatrix}1, & \mathfrak{e}|f\\ e, & \mathfrak{e}\nmid f\end{smallmatrix}\right\}\Bigr).$$

□

Combining Propositions 3.16, 3.18 and 3.19 proves Proposition 3.10 in Cases (3C) and (3D).

3.iv.3. *(Case 3M) E/K has potentially multiplicative reduction.* In view of Lemma 3.13, it suffices to prove the following

Claim. Suppose $f_{F/K}$ is a power of 2. Then $\omega\sim1\sim a$ and $c_v\sim d$, and hence $C_v\sim\mathfrak{D}_V$.

Proposition 3.20. *$\omega\sim1\sim a$.*

Proof. As V is a C_2-representation and C_2 has no relations, $a\sim1$ by Theorem 2.36q. Also $\omega=(D,I,q^{\lfloor\frac{\mathfrak{e}}{2}\rfloor f})\sim1$, by the proof of $\mathfrak{e}=2,\delta=6$ case of Proposition 3.18. □

Proposition 3.21. *$c_v\sim d$.*

Proof. For $H<D$, the expression for $c_v(E/F^H)$ is given in Lemma 3.22 (note that $L=K(\sqrt{-6B})$ in its notation). Writing $e=e_{F^H/K}$, $f=f_{F^H/K}$, we have

	E/F^H	c_v	d	c_v/d
$L\subset F^H$	I_{ne} split	ne	$\frac{\lvert D\rvert}{ef}$	$\frac{n}{\lvert D\rvert}e^2f$
$L\not\subset F^H, 2\lvert e$	I_{ne} non-split	2	1	2
$L\not\subset F^H, 2\nmid e, f{=}1$	I_{ne}^*	$c_v(E/K)$	1	$c_v(E/K)$
$L\not\subset F^H, 2\nmid e, 2\lvert f$	I_{ne}^*	4	1	4

Write L^u and K^u for the maximal unramified extensions of L and K inside F, respectively. By Lemma 3.24, the function c_v/d (to $\mathbb{Q}^\times/\mathbb{Q}^{\times2}$) factors through

$$\mathrm{Gal}(L^u/K)\ =\ \mathrm{Gal}(L^u/K^u)\times\mathrm{Gal}(L^u/L)\ =\ \mathrm{C}_2\times\mathrm{C}_{2^k}.$$

By Theorem 2.36q, it suffices to prove that c_v/d is trivial on $\mathrm{Gal}(L^u/K)$-relations. A list of generating relations is given in Example 2.10 (with $u{=}1$ and $m{=}1$). These come from $\mathrm{C}_2{\times}\mathrm{C}_2$-subquotients, each with one relation (Example 2.3) and it is elementary to verify that c_v/d is trivial on these. □

3.iv.4. *Appendix: Local lemmas.*

Lemma 3.22. *Let $K'/K/\mathbb{Q}_l$ be finite extensions with $l \geq 5$, and let E/K be an elliptic curve with additive reduction,*

$$E: y^2 = x^3 + Ax + B, \qquad A, B \in K.$$

Write $\Delta = -16(4A^3 + 27B^2)$ for the discriminant of this model, $\eth$ for its K-valuation, and $e = e_{K'/K}$.

If E has potentially good reduction, then

$$\begin{array}{lcll} \gcd(\eth e, 12) = 2 & \Longrightarrow & c_v(E/K') = 1 & (\mathrm{II}, \mathrm{II}^*) \\ \gcd(\eth e, 12) = 3 & \Longrightarrow & c_v(E/K') = 2 & (\mathrm{III}, \mathrm{III}^*) \\ \gcd(\eth e, 12) = 4 & \Longrightarrow & c_v(E/K') = \begin{cases} 1, & \sqrt{B} \notin K' \\ 3, & \sqrt{B} \in K' \end{cases} & (\mathrm{IV}, \mathrm{IV}^*) \\ \gcd(\eth e, 12) = 6 & \Longrightarrow & c_v(E/K') = \begin{cases} 2, & \sqrt{\Delta} \notin K' \\ 1 \text{ or } 4, & \sqrt{\Delta} \in K' \end{cases} & (\mathrm{I}_0^*) \\ \gcd(\eth e, 12) = 12 & \Longrightarrow & c_v(E/K') = 1 & (\mathrm{I}_0). \end{array}$$

The extension $K'(\sqrt{B})/K'$ in the IV, IV* *cases and $K'(\sqrt{\Delta})/K'$ in the* I_0^* *case is unramified. In particular if K''/K' has odd residue degree and* $\gcd(\eth e_{K'/K}, 12) = \gcd(\eth e_{K''/K}, 12)$*, then $c_v(E/K') = c_v(E/K'')$.*

If E has potentially multiplicative reduction of type I_n^* *over K, then*

$$\begin{array}{lcll} 2 \nmid e, 2 \nmid n & \Longrightarrow & c_v(E/K') = \begin{cases} 2, & \sqrt{B} \notin K' \\ 4, & \sqrt{B} \in K' \end{cases} & (\mathrm{I}_{ne}^*) \\ 2 \nmid e, 2 | n & \Longrightarrow & c_v(E/K') = \begin{cases} 2, & \sqrt{\Delta} \notin K' \\ 4, & \sqrt{\Delta} \in K' \end{cases} & (\mathrm{I}_{ne}^*) \\ 2 | e, \sqrt{-6B} \notin K' & \Longrightarrow & c_v(E/K') = 2 & (\mathrm{I}_{ne} \textit{ non-split}) \\ 2 | e, \sqrt{-6B} \in K' & \Longrightarrow & c_v(E/K') = ne & (\mathrm{I}_{ne} \textit{ split}). \end{array}$$

The extension $K'(\sqrt{B})/K'$, $K'(\sqrt{\Delta})/K'$ or $K'(\sqrt{-6B})/K'$ corresponding to the case is unramified.

Proof. This follows from Tate's algorithm ([38], IV.9). □

Remark 3.23. Let K be a finite extension of $\mathbb{Q}_l$ with $l \geq 5$, and E/K an elliptic curve. Recall that $c_v(E/K)$ is the size of the Néron component group $E(K)/E_0(K)$. When E/K has additive reduction, this group is of order at most 4, and is isomorphic to the prime-to-l torsion in $E(K)$. (Use the standard exact sequence [37] VII.2.1 and note that multiplication-by-l is an isomorphism both on the formal group of E and on the reduced curve.) In particular, in the I_0^* case of the lemma, $c_v(E/K') = 1$ if and only if E/K' has trivial 2-torsion.

Lemma 3.24. *Suppose $L/K/\mathbb{Q}_l$ are finite extensions. For every divisor $m | e_{L/K}$ with $l \nmid m$, there exists a subfield M of L/K with $e_{M/K} = m$ and L/M totally ramified.*

Proof. Replacing K by its maximal unramified extension in L, we may assume that L/K is totally ramified. Let F be the Galois closure of L/K, and write $G = \mathrm{Gal}(F/K)$, $H = \mathrm{Gal}(F/L)$ and I for the inertia subgroup of G. Let N be the unique index m subgroup of I. We claim that $M = F^{NH}$ will do.

Since $e_{M/K} = [I : I \cap NH]$ and $[I : N] = m$, it is enough to prove that $N = I \cap NH$. "$\subset$" is clear. Observe that every subgroup U of I whose index is divisible by m is contained in N. (This is clear if U contains the wild inertia subgroup $W \triangleleft I$, as I/W is cyclic; otherwise replace U by UW.) In particular, $m | e_{L/K} = [I : I \cap H]$ implies that $I \cap H \subset N$. Since N is characteristic in $I \triangleleft G$ and therefore normal in G, it follows that $I \cap NH \subset N$ as asserted. $\square$

Lemma 3.25. *Suppose $K/\mathbb{Q}_l$ is finite, $\mathfrak{e} = 2, 3, 4, 6$, and the size of the residue field of K is congruent to -1 modulo $\mathfrak{e}$. Then the compositum F of all totally ramified extensions of K of degree $\mathfrak{e}$ is a dihedral extension of degree $2\mathfrak{e}$. Specifically, $F = K'(\sqrt[\mathfrak{e}]{\pi})$ with π a uniformiser of K and K'/K quadratic unramified.*

Proof. For $\mathfrak{e} = 2$ this is elementary. Otherwise, $K(\mu_{\mathfrak{e}}) = K'$ and it suffices to prove that every totally ramified degree $\mathfrak{e}$ extension of K is contained in $K'(\sqrt[\mathfrak{e}]{\pi})$.

For $\mathfrak{e} = 3$ suppose L/K is cubic totally ramified. It cannot be Galois by local class field theory, since the units of K have no index 3 subgroups. So its Galois closure is an S_3-extension, which is tame and so contains $K' = K(\mu_3)$. By Kummer theory, LK'/K' is contained in the $\mathrm{C}_3 \times \mathrm{C}_3$-extension M of K' obtained by adjoining cube roots of all elements of K'. But it is easy to see that $\mathrm{Gal}(M/K) \cong \mathrm{C}_6 \ltimes \mathrm{C}_3$ has a unique S_3-quotient, so $LK' = K'(\sqrt[\mathfrak{e}]{\pi})$ and $L \subset K'(\sqrt[\mathfrak{e}]{\pi})$ as asserted.

For $\mathfrak{e} = 4$, every totally ramified quartic extension of K has a quadratic subfield by Lemma 3.24, so there are at most 4 of them by the $\mathfrak{e} = 2$ case. Since in this case $K'(\sqrt[\mathfrak{e}]{\pi})$ has 4 totally ramified subfields corresponding to the non-normal subgroups of order 2 in D_8, they are all contained in it.

For $\mathfrak{e} = 6$ the assertion follows from the $\mathfrak{e} = 2$ and $\mathfrak{e} = 3$ cases (apply Lemma 3.24 for $m = 2$ and $m = 3$). $\square$

3.v. **Case (4): Semistable abelian varieties.**

3.v.1. *Review of abelian varieties with semistable reduction.* Let K be a finite extension of $\mathbb{Q}_l$, let A/K be an abelian variety and take a prime $p \neq l$. Fix a finite Galois extension L/K where A acquires split semistable reduction. By the work of Raynaud ([27], [13] §9), there is a smooth commutative group scheme $\mathcal{A}/\mathcal{O}_L$, which is an extension

$$0 \longrightarrow \mathcal{T} \longrightarrow \mathcal{A} \longrightarrow \mathcal{B} \longrightarrow 0,$$

with $\mathcal{T}/\mathcal{O}_L$ a split torus and $\mathcal{B}/\mathcal{O}_L$ an abelian scheme, and such that $\mathcal{A} \otimes (\mathcal{O}_L/m_L^i)$ is the identity component of the Néron model of A over $\mathcal{O}_L$ base changed to $\mathcal{O}_L/m_L^i$. These properties characterise $\mathcal{A}$ up to a unique isomorphism. In particular, the group $\mathrm{Gal}(L/K)$ acts naturally on $\mathcal{T}, \mathcal{A}$ and $\mathcal{B}$. The character group of $\mathcal{T}$ is a finite free $\mathbb{Z}$-module with an action of $\mathrm{Gal}(L/K)$, and we denote it $X(\mathcal{T})$.

The dual abelian variety A^t/K also has split semistable reduction over L, and there is a sequence as above with $\mathcal{T}^*, \mathcal{A}^*$ and $\mathcal{B}^* \cong \mathcal{B}^t$ ([13] Thm. 5.4). Raynaud constructs a canonical map $X(\mathcal{T}^*) \hookrightarrow \mathcal{A}(L)$, inducing an isomorphism of $\mathrm{Gal}(\bar{K}/K)$-modules

$$A(\bar{K}) \cong \mathcal{A}(\bar{K})/X(\mathcal{T}^*),$$

which generalises Tate's parametrisation for elliptic curves. (The $\mathrm{Gal}(\bar{K}/K)$-action on $\mathcal{A}(\bar{K})$ comes from the Galois action of $\mathrm{Gal}(\bar{K}/L)$ and the geometric action of $\mathrm{Gal}(L/K)$; see [3] §2.9.) From this description, there are exact sequences for the p-adic Tate modules of the generic fibres over L,

$$\begin{array}{l} 0 \longrightarrow T_p(\mathcal{T}_L) \longrightarrow T_p(\mathcal{A}_L) \longrightarrow T_p(\mathcal{B}_L) \longrightarrow 0 \\ 0 \longrightarrow T_p(\mathcal{A}_L) \longrightarrow T_p(A) \longrightarrow X(\mathcal{T}^*) \otimes \mathbb{Z}_p \longrightarrow 0. \end{array}$$

In particular, $T_p(A)$ has a filtration with graded pieces

$$\mathrm{gr}_0 = X(\mathcal{T}^*) \otimes \mathbb{Z}_p, \quad \mathrm{gr}_1 = T_p(\mathcal{B}_L), \quad \mathrm{gr}_2 = \mathrm{Hom}(X(\mathcal{T}), \mathbb{Z}_p(1)).$$

Now suppose A/K has *semistable* reduction. The reduction becomes split semistable over some finite unramified extension of K, and we take L to be the smallest such field; so now $\mathrm{Gal}(L/K)$ is cyclic, generated by Frobenius. To describe the Tamagawa number $c_v(A/K)$ and the action of inertia on $T_p(A)$ we use the monodromy pairing

$$X(\mathcal{T}^*) \times X(\mathcal{T}) \longrightarrow \mathbb{Z}.$$

This is a non-degenerate $\mathrm{Gal}(L/K)$-invariant pairing, and induces a Galois-equivariant inclusion of lattices

$$N : X(\mathcal{T}^*) \hookrightarrow \mathrm{Hom}(X(\mathcal{T}), \mathbb{Z}).$$

These have the same $\mathbb{Z}$-rank, so N has finite cokernel. Moreover, N is covariantly functorial with respect to isogenies of semistable abelian varieties. Any polarisation on A gives a map $X(\mathcal{T}^*) \to X(\mathcal{T})$, and the induced pairing

$$X(\mathcal{T}^*) \times X(\mathcal{T}^*) \longrightarrow \mathbb{Z}$$

is symmetric ([13] §10.2). In particular, if A is principally polarised, we get a perfect Galois-equivariant symmetric pairing

$$\mathrm{coker}\, N \times \mathrm{coker}\, N \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

If K'/K is a finite extension, then $X(\mathcal{T})$ and $X(\mathcal{T}^*)$ remain the same modules (restricted to $\mathrm{Gal}(LK'/K') \subset \mathrm{Gal}(L/K)$) by uniqueness of Raynaud parametrisation. The map N becomes $e_{K'/K}N$, see [13] 10.3.5.

The $\mathrm{Gal}(\bar{K}/K)$-module $\mathrm{gr}_2 \oplus \mathrm{gr}_1 \oplus \mathrm{gr}_0$ is unramified and semisimple, so it is a semisimplification of T_pA. With respect to this filtration, the inertia group acts on T_pA by

$$I_{\bar{K}/K} \ni \sigma \quad \longmapsto \quad \begin{pmatrix} 1 & 0 & t_p(\sigma)N \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{Aut}\, T_p(A)$$

with $t_p : I_{\bar{K}/K} \to \mathbb{Z}_p(1)$ defined by $\sigma \mapsto \sigma(\pi_K^{1/p^n})/\pi_K^{1/p^n} \in \mu_{p^n}$ for any uniformiser π_K of K ([13] §§9.1–9.2).

Let Φ be the group scheme of connected components of the special fibre of the Néron model of $A/\mathcal{O}_K$. It is an étale group scheme over the residue field k of K, so $\Phi(k) = \Phi(\bar{k})^{\mathrm{Gal}(\bar{k}/k)}$ consists of components defined over k. As K is complete and k is perfect, by [2] Lemma 2.1 the natural reduction map $A(K) \to \Phi(k)$ is onto, so $c_v(A/K) = |\Phi(k)|$. Finally, by [13] Thm. 11.5, $\Phi = \operatorname{coker} N$ as groups with $\mathrm{Gal}(\bar{k}/k) = \mathrm{Gal}(K^{un}/K)$-action, so

$$c_v(A/K) = |(\operatorname{coker} N)^{\mathrm{Gal}(L/K)}|.$$

3.v.2. *Local root numbers for twists of semistable abelian varities.*

Proposition 3.26. *Suppose A/K is semistable, let F/K be a finite Galois extension containing L, and τ a complex representation of* $\mathrm{Gal}(F/K)$*. Then*

$$w(A/K, \tau) = w(\tau)^{2\dim A}(-1)^{\langle \tau, X(\mathcal{T}^*)\rangle}.$$

Proof. Let $H^1(A) = H^1_{\text{ét}}(A, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{C} = \mathrm{Hom}(T_pA \otimes \mathbb{C}, \mathbb{C})$ for some $p \neq l$, and let $H^1(A)_{\mathrm{ss}}$ be its semisimplification. Write $V = X(\mathcal{T}^*) \otimes \mathbb{Q}$, and $\operatorname{sgn} z = z/|z|$ for $z \in \mathbb{C}^\times$. By the unramified twist formula [39] 3.4.6,

$$w((H^1(A)_{\mathrm{ss}}) \otimes \tau) = w(\tau)^{2\dim A} \operatorname{sgn}\det(\mathrm{F}|H^1(A)_{\mathrm{ss}})^\nu$$

for some integer ν and $\mathrm{F} = \mathrm{Frob}^{-1}_{\bar{K}/K}$. Since $\det(H^1(A))$ is a power of the cyclotomic character, this expression is just $w(\tau)^{2\dim A}$. By [39] 4.2.4,

$$\begin{aligned}
&w(A/K, \tau) = w(H^1(A) \otimes \tau)\\
&= w((H^1(A)_{\mathrm{ss}}) \otimes \tau) \tfrac{\operatorname{sgn}\det(-\mathrm{F}|((H^1(A)_{\mathrm{ss}}) \otimes \tau)^I)}{\operatorname{sgn}\det(-\mathrm{F}|((H^1(A) \otimes \tau)^I)}\\
&= w(\tau)^{2\dim A} \operatorname{sgn}\det(-\mathrm{F}|\mathrm{gr}^*_2 \otimes \tau^I)\\
&= w(\tau)^{2\dim A} \operatorname{sgn}\det(-\mathrm{F}|V \otimes \tau^I)\\
&= w(\tau)^{2\dim A}(-1)^{\dim V \dim \tau^I} \det(\mathrm{F}|V)^{\dim \tau^I} \det(\mathrm{F}|\tau^I)^{\dim V},
\end{aligned}$$

where the penultimate equality again comes from [39] 3.4.6. If η denotes the unramified character $\mathrm{F} \mapsto -1$, we have

$$(-1)^{\dim V} = (-1)^{\langle \mathbf{1}, V\rangle + \langle \eta, V\rangle}, \qquad \det(\mathrm{F}|V) = (-1)^{\langle \eta, V\rangle}$$

and similarly for τ^I in place of V, as they are both self-dual and unramified. Now a trivial computation shows that

$$(-1)^{\langle \tau, V\rangle} = (-1)^{\langle \tau^I, V\rangle} = (-1)^{\langle \mathbf{1}, \tau^I\rangle\langle \mathbf{1}, V\rangle + \langle \eta, \tau^I\rangle\langle \eta, V\rangle}$$

coincides with $w(A/K, \tau)/w(\tau)^{2\dim A}$, as asserted. □

3.v.3. *Tamagawa numbers for semistable abelian varieties.*

Proposition 3.27. *Suppose A/K is semistable and principally polarised, and set $V = X(\mathcal{T}^*) \otimes \mathbb{Q}$. Let F/K be a finite Galois extension containing L,*

and write $D=\mathrm{Gal}(F/K)$*,* $I\triangleleft D$ *for its inertia subgroup and* $\mathrm{F}=\mathrm{Frob}_{L/K}^{-1}$*. As functions from the Burnside ring of* D *to* $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$*,*

$$C_v=c_v\sim\big(D,I,e^{\dim V^{\mathrm{F}^f}}\big)\sim\mathfrak{D}_V$$

(up to factors of 2 in Case (4ex)*).*

Proof. The Néron model of $A/\mathcal{O}_K$ commutes with base change as A is semistable, so the minimal exterior form ω remains minimal in extensions of K, and $C_v=c_v$.

As V is unramified,

$$\mathfrak{D}_V=(H\mapsto\det(\tfrac{1}{|H|}\langle,\rangle|V^H))=\big(D,I,(\tfrac{|D|}{ef})^{\dim V^{\mathrm{F}^f}}\det(\langle,\rangle|V^{\mathrm{F}^f})\big)$$

which is $\sim\big(D,I,e^{\dim V^{\mathrm{F}^f}}\big)$ by Theorem 2.36f. This proves the last $\sim$.

As explained above, $c_v=\big(D,I,(\operatorname{coker}eN)^{\mathrm{F}^f}\big)$. So it remains to prove that $\big(D,I,\phi(e,f)\big)\sim 1$, where

$$\phi(e,f)=\big|(\operatorname{coker}eN)^{\mathrm{F}^f}\big|\,e^{-\dim V^{\mathrm{F}^f}}\quad\in\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\,.$$

Claim. The function ϕ satisfies:

(1) $\phi(e,pf)=\phi(e,f)$ for p odd.
(2) $\phi(e,4f)=\phi(e,2f)$.
(3) $\phi(e,2)=|\operatorname{coker}N|$.
(4) $\phi(2^ke,f)=\phi(2^k,f)$ for e odd.
(5) $\phi(e,f)=2^{\lambda_{e,f}}\phi(1,f)$ for some $\lambda_{e,f}\in\mathbb{Z}$.

Before verifying the claim, let us use these properties to complete our proof. Note that the asserted formula already holds up to multiples of 2 by (5) and Theorem 2.36f.

Let $W\triangleleft I$ be the wild inertia subgroup. Then

$$\begin{array}{rcl}\big(D,I,\phi(e,f)\big) & \overset{(1,2)}{=} & \Big(D,I,\Big\{\begin{smallmatrix}\phi(e,2), & 2|f\\ \phi(e,1), & 2\nmid f\end{smallmatrix}\Big\}\Big)\overset{(3)}{=}\Big(D,I,\Big\{\begin{smallmatrix}|\operatorname{coker}N|, & 2|f\\ \phi(e,1), & 2\nmid f\end{smallmatrix}\Big\}\Big)\\ & \overset{2.36\mathrm{f}}{\sim} & \Big(D,I,\Big\{\begin{smallmatrix}1, & 2|f\\ \phi(e,1), & 2\nmid f\end{smallmatrix}\Big\}\Big)\\ & \overset{2.36\mathrm{d}}{\sim} & \big(I,I,\phi(e,1)\big)\overset{2.36\mathrm{r}}{\sim}\big(I,W,\phi(ef,1)\big).\end{array}$$

If K has odd residue characteristic, then the wild inertia group W has odd order and $\big(I,W,\phi(ef,1)\big)=\big(I,W,\phi(f,1)\big)\sim 1$ by (4) and Theorem 2.36f. Suppose K has residue characteristic 2. Then $[I:W]$ is odd, and

$$\big(I,W,\phi(ef,1)\big)\overset{(4)}{=}\big(I,W,\phi(e,1)\big)\overset{2.36\mathrm{d}}{\sim}\big(W,W,\phi(e,1)\big).$$

If W is cyclic, this is ~ 1 as asserted, since W has no relations. If $2\nmid[L\!:\!K]$, then F and F^2 generate the same group, so

$$\big(W,W,\phi(e,1)\big)=\big(W,W,\phi(e,2)\big)\overset{(3)}{=}\big(W,W,|\operatorname{coker}N|\big)\overset{2.36\mathrm{f}}{\sim}1\,.$$

Otherwise we are in case (4ex) and we claim nothing about factors of 2. $\square$

3.28. *Proof of claim.* This is a purely module-theoretic statement about the G-modules $X(\mathcal{T}^*) \hookrightarrow \mathrm{Hom}(X(\mathcal{T}), \mathbb{Z})$ and the monodromy pairing. Suppose $G = \langle \mathrm{F} \rangle$ is a finite cyclic group, and $N : M' \hookrightarrow M$ is an inclusion of $\mathbb{Z}G$-lattices of the same (finite) rank. Furthermore, suppose for every $e \geq 1$ there is a perfect symmetric G-invariant pairing

$$\langle , \rangle_e : \; M/eM' \times M/eM' \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Then the function

$$\phi(e, f) = \left|(\mathrm{coker}\, eN)^{\mathrm{F}^f}\right| e^{-\mathrm{rk}\, M^{\mathrm{F}^f}} \quad \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

satisfies (1)–(5):

(1) As $M \otimes \mathbb{Q}$ is a self-dual representation (every rational representation is self-dual), $\mathrm{rk}\, M^{\mathrm{F}^f} \equiv \mathrm{rk}\, M^{\mathrm{F}^{pf}} \mod 2$. Write $U = M/eM'$ and $Z = \mathrm{F}^f$. Then

$$(m, n) = \langle Zm - Z^{-1}m, n \rangle_e$$

defines an alternating pairing $U^{Z^p} \times U^{Z^p} \longrightarrow \mathbb{Q}/\mathbb{Z}$ whose left kernel is $U^{Z^2} \cap U^{Z^p} = U^Z$. So it is a perfect alternating pairing on U^{Z^p}/U^Z, hence this group has square order.

(2) Again $M \otimes \mathbb{Q}$ is self-dual, so $\mathrm{rk}\, M^{\mathrm{F}^{4f}} \equiv \mathrm{rk}\, M^{\mathrm{F}^{2f}} \mod 2$. Next, the above formula for $(,)$ with $Z = \mathrm{F}^f$ defines an alternating pairing $U^{\mathrm{F}^{4f}} \times U^{\mathrm{F}^{4f}} \to \mathbb{Q}/\mathbb{Z}$ whose left kernel is $U^{Z^2} \cap U^{Z^4} = U^{Z^2}$, so U^{Z^4}/U^{Z^2} has square order.

(3) By (1) and (2), $\phi(e, 2) = \phi(e, |G|) = |M/eM'| e^{\mathrm{rk}\, M} = |M/M'|$.

(4) Replacing F by F^f we may assume $f = 1$. We may also suppose that F has order a power of 2 by (1). It suffices to show that in the exact sequence

$$0 \longrightarrow \Big(\frac{2^k M'}{2^k eM'}\Big)^{\mathrm{F}} \longrightarrow \Big(\frac{M}{2^k eM'}\Big)^{\mathrm{F}} \longrightarrow \Big(\frac{M}{2^k M'}\Big)^{\mathrm{F}} \longrightarrow H^1\Big(G, \frac{2^k M'}{2^k eM'}\Big)$$

the first term has order $e^{\mathrm{rk}\, M^{\mathrm{F}}}$ and the last one is 0. Because $\frac{2^k M'}{2^k eM'} \cong \frac{M'}{eM'}$, it has odd order and hence has trivial H^1. Next, from the long exact cohomology sequence for the multiplication by e map on M' we extract

$$0 \longrightarrow \frac{M'^{\mathrm{F}}}{eM'^{\mathrm{F}}} \longrightarrow \Big(\frac{M'}{eM'}\Big)^{\mathrm{F}} \longrightarrow H^1(G, M')[e].$$

The last term is killed by $|G|$ and e, and is therefore 0. So

$$\Big|\Big(\frac{2^k M'}{2^k eM'}\Big)^{\mathrm{F}}\Big| = \Big|\Big(\frac{M'}{eM'}\Big)^{\mathrm{F}}\Big| = \Big|\frac{M'^{\mathrm{F}}}{eM'^{\mathrm{F}}}\Big| = e^{\mathrm{rk}\, M^{\mathrm{F}}},$$

as required.

(5) By (4), we only need to show that $\phi(2^k, f)$ differs from $\phi(1, f)$ by a power of 2. But the first and the last term in the exact sequence

$$\Big(\frac{M'}{2^k M'}\Big)^{\mathrm{F}^f} \longrightarrow \Big(\frac{M}{M'}\Big)^{\mathrm{F}^f} \longrightarrow \Big(\frac{M}{2^k M'}\Big)^{\mathrm{F}^f} \longrightarrow H^1\Big(\langle F^f \rangle, \frac{2M'}{2^k M'}\Big)$$

are killed by 2^k, and the result follows from the definition of ϕ. $\square$

Remark 3.29. If we could also prove that $\phi(4,1)=\phi(2,1)$ for ϕ as in 3.28, we would be able to deal with the exceptional case (4ex) of Theorem 3.2 using an argument similar to that in §3.iii.3. It would then remove the ugly restriction on the reduction type for $p=2$ in Theorem 1.6(b). (Embarassingly, this is purely a problem about $\mathbb{Z}\mathrm{C}_n$-modules.)

Combining Propositions 3.26 and 3.27 completes Case (4) of Proposition 3.10 and the proof of Theorem 3.2.

4. Applications to the parity conjecture

We now have a machine that, when supplied with a relation Θ between permutation representations, confirms the p-parity conjecture for the twists of A/K by the representations $\tau \in \mathbf{T}_{\Theta,p}$ coming from regulator constants. We turn to a class of Galois groups where these are enough to say something about essentially all twists for some p.

Specifically, we concentrate on Galois groups $G=\mathrm{Gal}(F/K)$ that have a normal p-subgroup P. The type of results that we aim for is that knowing p-parity for all G/P-twists is sufficient to establish it for all G-twists. In particular, we prove Theorems 1.11 and 1.12.

Apart from the machine itself (Theorem 1.6) the proofs rely only on group theory and basic parity properties of Selmer ranks and root numbers. Roughly speaking, we may consider any functions, such as $\tau \mapsto w(A/K,\tau)$ or $\tau \mapsto (-1)^{\langle \tau, \mathcal{X}_p(A/F)\rangle}$ that satisfy "self-duality" and "inductivity" as in Proposition A.2(1,2). If two such functions agree on G/P-twists and on the $\tau \in \mathbf{T}_{\Theta,p}$ for those Θ that come from dihedral subquotients, this sometimes forces them to agree on all orthogonal G-twists, or at least on those twists that correspond to intermediate fields.

We will not formulate the results of this section in this language. However, to be able in principle to extend them to a larger class of abelian varieties, we axiomatise the minimal compatibility requirements:

Hypothesis 4.1 (Compatibility in dihedral subquotients)**.** Let F/K be a Galois extension of number fields, A/K an abelian variety and p a prime number. We demand the following[2]: whenever $N \triangleleft U$ are subgroups of $\mathrm{Gal}(F/K)$ with $U/N \cong \mathrm{D}_{2p^n}$ and $\tau = \sigma \oplus \mathbf{1} \oplus \det\sigma$ for some 2-dimensional representation σ of U/N,

$$(-1)^{\langle \tau, \mathcal{X}_p(A/F^N)\rangle_U} = w(A/F^U, \tau).$$

In other words, the p-parity conjecture holds for the twists by all such τ. (Recall that we regard $\mathrm{C}_2 \times \mathrm{C}_2$ as a dihedral group as well.)

[2] For odd p, the hypothesis may be relaxed to subquotients $U/N \cong \mathrm{D}_{2p}$; this follows from the recent invariance result of Rohrlich (Prop. A.2(5) or [32] Thms. 1,2).

Theorem 4.2. *Hypothesis 4.1 holds for*

(1) *(any p) all elliptic curves over K whose primes of additive reduction above 2 and 3 have cyclic decomposition groups in F/K (e.g. are unramified).*
(2) *($p \neq 2$) all principally polarised abelian varieties over K whose primes of unstable reduction have cyclic decomposition groups in F/K (e.g. all semistable principally polarised abelian varieties).*
(3) *($p = 2$) abelian varieties over K with a principal polarisation coming from a K-rational divisor, whose primes of unstable reduction have cyclic decomposition groups in F/K, and with split semistable reduction at those primes above 2 that have non-cyclic wild inertia groups in F/K.*

Proof. Apply Theorem 1.6 to the relations in Examples 2.21 and 2.22. □

Throughout the section we implicitly use that $\mathcal{X}_p$ behaves in an "étale" fashion: for $K \subset L \subset F$ an intermediate field, $\mathcal{X}_p(A/L) = \mathcal{X}_p(A/F)^{\mathrm{Gal}(F/L)}$ (see e.g. [6] Lemma 4.14). We occasionally say that "p-parity holds" for A/L or for a twist of A by τ, referring to Conjectures 1.2a, 1.2b.

4.i. **Parity over fields.**

Theorem 4.3. *Let A, $p \neq 2$ and F/K satisfy Hypothesis 4.1. Suppose $P \triangleleft \mathrm{Gal}(F/K)$ is a p-subgroup. If the p-parity conjecture holds for A over all subfields of F^P/K, then it holds over all subfields of F/K.*

Proof. Write $G = \mathrm{Gal}(F/K)$ and V for $Z(P)[p]$, the p-elementary part of the centre of P. We may assume $P \neq 1$, so V is non-trivial. As V is characteristic in P, it is normal in G. We need to prove p-parity for A/F^H for all subgroups H of G, and it holds when $P \subset H$ by assumption. We use induction on $|G|$ to reduce G and H to small explicit groups. Thus, assume the theorem holds for all proper subquotients $|\mathrm{Gal}(F'/K')| < |\mathrm{Gal}(F/K)|$.

Fix $H \lneq G$. Suppose there is a subgroup $1 \neq U \triangleleft G$ with $U \subset P$ and $HU \neq G$. Applying the theorem to $P/U \triangleleft \mathrm{Gal}(F^U/K)$, p-parity holds over all subfields of F^U/K, including the intermediate fields of F^U/F^{HU}. Applying it again to $U \triangleleft \mathrm{Gal}(F/F^{HU})$ shows that p-parity holds over the subfields of F/F^{HU}, in particular F^H.

Hence we may assume that whenever $U \triangleleft G$ is a subgroup of P, either $U = 1$ or $HU = G$. In particular, $HV = G$ as $V \triangleleft G$ is non-trivial. Furthermore, $H \cap V = 1$ because it is normal in $HV = G$ and $H(H \cap V) = H \neq G$. It follows that $G \cong H \ltimes V$.

Moreover, $P = (P \cap H) \ltimes V$, as P contains V. The two constituents commute, so this is a direct product and $V = Z(P)[p] = Z(P \cap H)[p] \times V$. So $P \cap H = 1$, and hence $P = V$.

Finally, we may assume that the action of H on V by conjugation is faithful. Otherwise let $W = \ker(H \to \mathrm{Aut}\, V)$ and note that $W \triangleleft H$, so

$W \lhd HV = G$. By induction, p-parity holds over all subfields of F^W/K, in particular over F^H.

We are reduced to the case

$$G = H \ltimes \mathbb{F}_p^k \quad \text{with} \quad H < \mathrm{GL}_k(\mathbb{F}_p) \qquad \text{(an affine linear group)},$$

where we need to show that p-parity for A/F^H follows from p-parity over the subfields of $F^{\mathbb{F}_p^k}/K$.

The group G acts on the one-dimensional complex characters of $\mathbb{F}_p^k$ by conjugation. Let $\{\chi_i\}$ be a set of representatives for the orbits, and let $S_i < G$ be the stabiliser of χ_i. Extend χ_i to a character $\tilde{\chi}_i$ of S_i by $\tilde{\chi}_i(hv) = \chi_i(v)$ for $h \in S_i \cap H$ and $v \in \mathbb{F}_p^k$. The representations $\mathrm{Ind}_{S_i}^G \tilde{\chi}_i$ are irreducible and distinct ([36] §8.2), and we observe that

$$\mathbb{C}[G/H] \;\cong\; \bigoplus_i \mathrm{Ind}_{S_i}^G \tilde{\chi}_i.$$

Indeed, both have dimension p^k, so it is enough to check that each term on the right is a consituent of $\mathbb{C}[G/H]$; but

$$\begin{array}{rcll}
\langle \mathbb{C}[G/H], \mathrm{Ind}_{S_i}^G \tilde{\chi}_i \rangle & = & \langle \mathbf{1}_H, \mathrm{Res}_H \mathrm{Ind}_{S_i}^G \tilde{\chi}_i \rangle & \text{(Frobenius reciprocity)} \\
& \geq & \langle \mathbf{1}_H, \mathrm{Ind}_{S_i \cap H}^H \mathrm{Res}_{S_i \cap H} \tilde{\chi}_i \rangle & \text{(Mackey's formula)} \\
& = & \langle \mathbf{1}_H, \mathrm{Ind}_{S_i \cap H}^H \mathbf{1}_{S_i \cap H} \rangle & \text{(definition of } \tilde{\chi}_i\text{)} \\
& = & \langle \mathrm{Res}_{S_i \cap H} \mathbf{1}_H, \mathbf{1}_{S_i \cap H} \rangle = 1 & \text{(Frobenius reciprocity).}
\end{array}$$

Now consider

$$\Sigma = \big\{ i \;\big|\; \mathrm{Ind}_{S_i}^G \tilde{\chi}_i \text{ self-dual} \big\} = \big\{ i \;\big|\; \chi_i^{\pm 1} \text{ belong to the same } H\text{-orbit} \big\}.$$

For $i \in \Sigma$ let M_i consist of those elements of G that take χ_i to $\chi_i^{\pm 1}$, and let $\psi_i = \mathrm{Ind}_{S_i}^{M_i} \tilde{\chi}_i$. Computing modulo 2,

$$\begin{array}{rcll}
\langle \mathbf{1}_H, \mathcal{X}_p(A/F) \rangle & = & \langle \mathbb{C}[G/H], \mathcal{X}_p(A/F) \rangle & \text{(Frobenius reciprocity)} \\
& \equiv & \sum_{i \in \Sigma} \langle \mathrm{Ind}_{S_i}^G \tilde{\chi}_i, \mathcal{X}_p(A/F) \rangle & \text{(Self-duality of } \mathcal{X}_p\text{)} \\
& \equiv & \sum_{i \in \Sigma} \langle \psi_i, \mathcal{X}_p(A/F) \rangle & \text{(Frobenius reciprocity).}
\end{array}$$

The same computation for the root numbers (using A.2(1,2)) shows that $w(A/F^H) = \prod_i w(A/F^{M_i}, \psi_i)$. So, it suffices to prove that

$$(-1)^{\langle \psi_i, \mathcal{X}_p(A/F) \rangle} = w(A/F^{M_i}, \psi_i).$$

If $\chi_i = \mathbf{1}$, then $S_i = G$, $\psi_i = \mathbf{1}$ and this p-parity holds by assumption. Otherwise, $\chi_i \neq \chi_i^{-1}$ as p is odd, and ψ_i factors through the D_{2p}-subquotient $M_i/\ker \tilde{\chi}_i$. In this case we know p-parity over its two bottom fields F^{S_i} and F^{M_i}, so it also holds for the twist of A/F^{M_i} by ψ_i (Hypothesis 4.1). $\square$

Theorem 4.4. *Let $A, p=2$ and F/K satisfy Hypothesis 4.1. Suppose that the Sylow 2-subgroup P of* $\mathrm{Gal}(F/K)$ *is normal. If the* 2*-parity conjecture holds for A over K and its quadratic extensions in F, then it holds over all subfields of F/K.*

Proof. Write $G=\mathrm{Gal}(F/K)$ and pick $H<G$. We prove p-parity for A/F^H.

`Step 1: Suppose` G `is a 2-group.`

There is a descending chain of subgroups $G=U_1\supset\ldots\supset U_n=H$ with all inclusions of index 2. We show by induction that 2-parity holds over all quadratic extensions of F^{U_i} in F. For $i=1$ this is true by assumption. Suppose this is true for $i-1$, and let L/F^{U_i} be a quadratic extension inside F. The Galois closure of the quartic extension $L/F^{U_{i-1}}$ has Galois group C_4, $\mathrm{C}_2\times\mathrm{C}_2$ or D_8, as it is a 2-group. In all cases, 2-parity over quadratic extensions of $F^{U_{i-1}}$ implies 2-parity for all orthogonal twists of this Galois group, in particular parity over L (for C_4 see Corollary A.3(1,2); for D_8 this is Hypothesis 4.1.)

`Step 2: General case.`

As $F^H/F^{H\cap P}$ is Galois of odd degree, 2-parity for A/F^H is equivalent to that for $A/F^{H\cap P}$ by Corollary A.3(3). Since P is a 2-group, by Step 1 it suffices to establish 2-parity over F^P and its quadratic extensions in F.

Let $\Phi\triangleleft P$ be its Frattini subgroup, so $P/\Phi\cong\mathbb{F}_2^k$ is its largest 2-elementary quotient. As Φ is characteristic in P, it is normal in G, and F^Φ/K is Galois. (F^Φ is the compositum of all quadratic extensions of F^P in F.) Replacing F by F^Φ we may assume that $\Phi=0$ and $P=\mathbb{F}_2^k$, so by the Schur-Zassenhaus theorem $G\cong U\ltimes\mathbb{F}_2^k$ with U of odd order.

We want to prove 2-parity for all twists of A/F^P by characters $\chi:\mathbb{F}_2^k\to\mathbb{C}^\times$. Write L_χ for $F^{\ker\chi}$ for such χ; so $[L_\chi:F^P]\le 2$.

As F^P/K is Galois of odd degree, 2-parity holds over $L_{\mathbf{1}}=F^P$, equivalently for the twist of A/F^P by $\mathbf{1}$. More generally, G acts on characters of $\mathbb{F}_2^k$ by conjugation, and if $\chi\ne\mathbf{1}$ is G-invariant, then L_χ/K is Galois with Galois group $U\times\mathrm{C}_2$. In this case, L_χ is an odd degree Galois extension of a quadratic extension of K in F, so again 2-parity holds over L_χ and hence for the twist of A/F^P by χ.

Now pick a general non-trivial $\chi=\chi_1$ and let $\{\chi_i\}_{1\le i\le n}$ be the complete set of its conjugates under G. The L_i are conjugate fields, so the 2-parity conjecture for the twist by χ is equivalent to that for any of the χ_i. As the orbit size n is odd, it suffices to check 2-parity for the twist of A/F^P by $\oplus_i\chi_i$.

Applying Hypothesis 4.1 in $\mathrm{C}_2\times\mathrm{C}_2$-extensions of F^P, 2-parity holds for the twist by $\mathbf{1}\oplus\phi\oplus\psi\oplus\phi\psi$ for any characters ϕ,ψ of $\mathbb{F}_2^k$. Taking a sum of such twists shows that 2-parity for $\oplus_i\chi_i$ is equivalent to 2-parity for $\mathbf{1}^{\oplus n}\oplus\prod\chi_i$. But this is a sum of G-invariant characters, for which 2-parity has already been established. $\square$

4.ii. **Parity for twists.**

Theorem 4.5. *Let A, p and F/K satisfy Hypothesis 4.1. Assume that the Sylow p-subgroup P of $G = \mathrm{Gal}(F/K)$ is normal and G/P is abelian. If the p-parity conjecture holds for A over K and its quadratic extensions in F, then it holds for all twists of A by orthogonal representations of G.*

Proof. Let τ be an orthogonal representation of G. By the analogue of Brauer's induction theorem for orthogonal representations [10] (2.1),

$$\tau = \bigoplus_i \mathrm{Ind}_{H_i}^G \rho_i^{\oplus n_i}$$

for some $H_i < G$, $n_i \in \mathbb{Z}$, and with ρ_i either (a) trivial or (b) $\chi \oplus \bar{\chi}$ with $\chi \neq \bar{\chi}$ one-dimensional or (c) a 2-dimensional irreducible that factors through a dihedral quotient of H_i.

By inductivity (Corollary A.3(2)), it suffices to prove that

$$(-1)^{\langle \rho_i, \mathcal{X}_p(A/F) \rangle_{H_i}} = w(A/F^{H_i}, \rho_i).$$

We distinguish between the three possibilities for ρ_i as above:

Case (a). As G/P is abelian, its only irreducible self-dual representations are those that factor through a C_2-quotient. By "self-duality" and "inductivity" (Corollary A.3(1,2)), the assumed parity over K and its quadratic extensions implies parity in all subfields of F^P/K. By Theorems 4.3 and 4.4, it implies parity in all subfields of F/K, in particular for A/F^{H_i}.

Case (b). The formula holds by Corollary A.3(1).

Case (c). Since the commutator of G is a p-group, the only dihedral subquotients it has are D_{2p^k}. By case (a), we know parity over F^{H_i} and its quadratic extensions in F, so Hypothesis 4.1 implies parity for all irreducible 2-dimensional representations of this subquotient. □

Remark 4.6. For elliptic curves, the assumption that the p-parity conjecture holds for E over K and its quadratic extensions in F is known in a number of cases. In particular ([1, 11, 14, 24, 25, 16, 6], [5, 3])

(1) if $K = \mathbb{Q}$;
(2) if E/K admits a rational p-isogeny, and for every prime $v|p$ of K,
   - ($p > 3$) E is semistable, potentially multiplicative or potentially ordinary at v, or acquires good supersingular reduction over an abelian extension of K_v.
   - ($p = 3$) E is semistable at v,
   - ($p = 2$) E is semistable, and not supersingular at v.

There are also results for modular abelian varieties over totally real fields [25, 17, 26] and a generalisation of (2) to abelian varieties with a suitable p^g-isogeny [3].

Remark 4.7. The assumption in Theorem 4.5 that G/P is abelian was only used to ensure that (a) p-parity holds in all intermediate fields of F^P/K, and (b) dihedral subquotients of G have the form D_{2p^n}. So the theorem extends to other extensions that satisfy (a) and (b), e.g. G nilpotent with $p=2$, or $G/P \cong$ (odd)×(abelian 2-group) with $p \neq 2$.

Example 4.8. Let $E/\mathbb{Q}$ be an elliptic curve, semistable at 2 and 3, and let $F=\mathbb{Q}(E[3])$. We claim that the 3-parity conjecture holds for E over all subfields of F, and consequently over all subfields of $F_n=\mathbb{Q}(E[3^n])$ by Theorems 4.2 and 4.3.

If either $F/\mathbb{Q}$ is abelian or $E/\mathbb{Q}$ admits a rational 3-isogeny, this is true by [7] Thm. 1.2 and [5] Thm. 2 respectively. Otherwise, $G=\mathrm{Gal}(F/\mathbb{Q})$ is one of the following subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$:

$$\mathrm{GL}_2(\mathbb{F}_3), \quad \mathrm{D}_8 \quad \text{or} \quad \mathrm{Sy}_{16} = \text{2-Sylow of } \mathrm{GL}_2(\mathbb{F}_3).$$

It is not hard to verify that in all three cases, the representations $\mathrm{Ind}_H^G \mathbf{1}_H$ for subgroups $H \subset \mathrm{C}_2\times\mathrm{C}_2$ (these correspond to fields where E acquires a 3-isogeny) and those with G/H abelian generate all orthogonal representations. Again, as the 3-parity conjecture is known for E/F^H for such H, this implies 3-parity for all intermediate fields.

The question whether 3-parity holds for all *twists* by self-dual representations of $\mathrm{Gal}(F_n/\mathbb{Q})$ is more subtle, as we do not have an analogue of Theorem 4.5 in this case. In fact, suppose that $G_2=\mathrm{Gal}(F_2/\mathbb{Q})\cong\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, i.e. as large as possible. Then there are precisely two irreducible orthogonal Artin representations $\tau_1,\tau_2: G_2\to\mathrm{GL}_6(\mathbb{C})$ that can be realised over $\mathbb{Q}_3(\sqrt{3})$ but not over $\mathbb{Q}_3$. It turns out that $\mathcal{C}_\Theta^{\mathbb{Q}_3}(\tau_1\oplus\tau_2)=1$ for every G_2-relation Θ, so the parity of $\langle\tau_i,\mathcal{X}_3(E/F_2)\rangle$ cannot be computed from regulator constants. (It can be computed for all other $\mathbb{C}G_2$-irreducible orthogonals.)

Appendix A: Basic parity properties

For the convenience of the reader, we record a few basic facts related to root numbers and the p-parity conjecture.

Lemma A.1 (Determinant formula)**.** *Let K be a local field and τ a continuous representation of the Weil group of K. Then*

$$w(\tau\oplus\tau^*)=\det(\tau)(\theta(-1))\ ,$$

where θ is the local reciprocity map on $K^\times$. For an abelian variety A/K,

$$w(A,\tau\oplus\tau^*)=1\ .$$

Proof. For the first statement see [29] p.145 or [39] 3.4.7. The second is an elementary computation using [39] 3.4.7, 4.2.4. ☐

Proposition A.2. *Let F/K be a Galois extension of number fields, and A/K an abelian variety. Write $\mathbf{A} = A(F) \otimes \mathbb{C}$ and $\mathcal{X} = \mathcal{X}_p(A/F)$. For an Artin representation $\tau : \mathrm{Gal}(F/K) \to \mathrm{GL}_n(\mathbb{C})$,*

(1) *(self-duality)*

$$\langle \tau, \mathbf{A} \rangle = \langle \tau^*, \mathbf{A} \rangle, \qquad \langle \tau, \mathcal{X} \rangle = \langle \tau^*, \mathcal{X} \rangle, \qquad w(A, \tau) = \overline{w(A, \tau^*)}.$$

(2) *(inductivity) If $K \subset L \subset F$ and $\tau = \mathrm{Ind}_{\mathrm{Gal}(F/L)}^{\mathrm{Gal}(F/K)} \rho$ then*

$$\langle \tau, \mathbf{A} \rangle = \langle \rho, \mathbf{A} \rangle, \quad \langle \tau, \mathcal{X} \rangle = \langle \rho, \mathcal{X} \rangle, \quad w(A/K, \tau) = w(A/L, \rho).$$

(3) *(odd degree base change) If F/K is Galois of odd degree, then*

$$\begin{array}{lcll} \mathrm{rk}(A/K) & \equiv & \mathrm{rk}(A/F) & \mod 2, \\ \dim \mathcal{X}_p(A/K) & \equiv & \dim \mathcal{X}_p(A/F) & \mod 2, \\ w(A/K) & = & w(A/F). & \end{array}$$

(4) *(orthogonality) If τ is symplectic, then $\langle \tau, \mathbf{A} \rangle$ is even and $w(A, \tau) = 1$.*

(5) *(equivariance) If τ is self-dual and τ' is a Galois conjugate of τ (i.e. their characters are Galois conjugate), then*

$$\langle \tau, \mathbf{A} \rangle = \langle \tau', \mathbf{A} \rangle, \quad w(A/K, \tau) = w(A/K, \tau').$$

Proof. (1) $\mathbf{A}$ is a rational representation, hence self-dual; $\mathcal{X}$ is self-dual as well by [7] Thm. 1.1. The root number formula follows from Lemma A.1.
(2) For $\mathbf{A}$ and $\mathcal{X}$ this is Frobenius reciprocity. The last formula is well-known; it is a consequence of inductivity in degree 0 of local ϵ-factors for Weil groups, [39] 4.2.4 and a simple determinant computation.
(3) Follows from (1), (2) and the fact that the only self-dual irreducible representation of $\mathrm{Gal}(F/K)$ is trivial.
(4) $\mathbf{A}$ is a rational representation, so $\langle \tau, \mathbf{A} \rangle$ is even; $w(A, \tau) = 1$ by [30] Prop. 8(iii) for elliptic curves, and by [33] Prop. 3.2.3 for abelian varieties.
(5) The statement for $\mathbf{A}$ is clear, as it is a rational representation. That for root numbers is clear from (4) in the symplectic case, and follows from [32] Thms 1,2 in the orthogonal case. □

Corollary A.3. *Suppose F/K is a Galois extension, and A/K an abelian variety. Then the p-parity conjecture*

(1) *holds for twists of A by representations of the form $\tau \oplus \tau^*$.*
(2) *holds for the twist of A/K by $\mathrm{Ind}_{\mathrm{Gal}(F/L)}^{\mathrm{Gal}(F/K)} \rho$ if and only if it holds for the twist of A/L by ρ, if $K \subset L \subset F$.*
(3) *holds for A/F if and only if it holds for A/K, if $[F : K]$ is odd.*

Acknowledgements. We would like to thank the referee for carefully reading the manuscript and for helpful comments.

References

[1] B. J. Birch, N. M. Stephens, The parity of the rank of the Mordell-Weil group, Topology 5 (1966), 295–299.

[2] S. Bosch, Q. Liu, Rational points of the group of components of a Néron model, Manuscripta Math. 98 (1999), no. 3, 275–293.

[3] J. Coates, T. Fukaya, K. Kato, R. Sujatha, Root numbers, Selmer groups and non-commutative Iwasawa theory, 2007, to appear in J. Alg. Geometry.

[4] P. Deligne, Valeur de fonctions L et périodes d'intégrales, in: Automorphic forms, representations and L-functions, Part 2 (ed. A. Borel and W. Casselman), Proc. Symp. in Pure Math. 33 (AMS, Providence, RI, 1979) 313–346.

[5] T. Dokchitser, V. Dokchitser, Parity of ranks for elliptic curves with a cyclic isogeny, J. Number Theory 128 (2008), 662–679.

[6] T. Dokchitser, V. Dokchitser, On the Birch–Swinnerton-Dyer quotients modulo squares, 2006, arxiv: math.NT/0610290, to appear in Annals of Math.

[7] T. Dokchitser, V. Dokchitser, Self-duality of Selmer groups, Math. Proc. Cam. Phil. Soc. 146 (2009), 257–267.

[8] V. Dokchitser, Root numbers of non-abelian twists of elliptic curves, with an appendix by T. Fisher, Proc. London Math. Soc. (3) 91 (2005), 300–324.

[9] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), no. 3, 349–366.

[10] A. Fröhlich, J. Queyrut, On the functional equation of the Artin L-function for characters of real representations, Invent. Math. 20 (1973), 125–138.

[11] R. Greenberg, On the Birch and Swinnerton-Dyer conjecture, Invent. Math. 72, no. 2 (1983), 241–265.

[12] R. Greenberg, Iwasawa theory, projective modules and modular representations, preprint, 2008.

[13] A. Grothendieck, Modèles de Néron et monodromie, LNM 288, Séminaire de Géométrie 7, Exposé IX, Springer-Verlag, 1973.

[14] L. Guo, General Selmer groups and critical values of Hecke L-functions, Math. Ann. 297 no. 2 (1993), 221–233.

[15] Y. Hachimori, O. Venjakob, Completely faithful Selmer groups over Kummer extensions, Documenta Mathematica, Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 443–478.

[16] B. D. Kim, The Parity Theorem of Elliptic Curves at Primes with Supersingular Reduction, Compos. Math. 143 (2007) 47–72.

[17] B. D. Kim, The parity conjecture over totally real fields for elliptic curves at supersingular reduction primes, preprint.

[18] K. Kramer, Arithmetic of elliptic curves upon quadratic extension. Trans. Amer. Math. Soc. 264 (1981), no. 1, 121–135.

[19] K. Kramer, J. Tunnell, Elliptic curves and local ϵ-factors, Compos. Math. 46 (1982), 307–352.

[20] B. Mazur, K. Rubin, Finding large Selmer ranks via an arithmetic theory of local constants, Annals of Math. 166 (2), 2007, 579–612.

[21] B. Mazur, K. Rubin, Growth of Selmer rank in nonabelian extensions of number fields, Duke Math. J. 143 (2008) 437–461.

[22] J. S. Milne, On the arithmetic of abelian varieties, Invent. Math. 17 (1972), 177–190.

[23] J. S. Milne, Arithmetic duality theorems, Perspectives in Mathematics, No. 1, 1986.

[24] P. Monsky, Generalizing the Birch–Stephens theorem. I: Modular curves, Math. Z., 221 (1996), 415–420.

[25] J. Nekovář, Selmer complexes, Astérisque 310 (2006).

[26] J. Nekovář, On the parity of ranks of Selmer groups IV, with an appendix by J.-P. Wintenberger, to appear in Compos. Math.

[27] M. Raynaud, Variétés abéliennes et géométrie rigide, Actes du congrès international de Nice 1970, tome 1, 473–477.
[28] D. Rohrlich, The vanishing of certain Rankin-Selberg convolutions, in: Automorphic forms and analytic number theory, Les publications CRM, Montreal, 1990, 123–133.
[29] D. Rohrlich, Elliptic curves and the Weil-Deligne group, in: Elliptic curves and related topics, 125–157, CRM Proc. Lecture Notes 4, Amer. Math. Soc., Providence, RI, 1994.
[30] D. Rohrlich, Galois Theory, elliptic curves, and root numbers, Compos. Math. 100 (1996), 311–349.
[31] D. Rohrlich, Scarcity and abundance of trivial zeros in division towers, J. Alg. Geometry 17 (2008), 643–675.
[32] D. Rohrlich, Galois invariance of local root numbers, preprint, 2008.
[33] M. Sabitova, Root numbers of abelian varieties and representations of the Weil-Deligne group, Ph. D. thesis, Univ. of Pennsylvania, 2005.
[34] M. Sabitova, Root numbers of abelian varieties, Trans. Amer. Math. Soc. 359 (2007), no. 9, 4259–4284.
[35] J.-P. Serre, Abelian l-adic Representations and Elliptic Curves, Addison-Wesley 1989.
[36] J.-P. Serre, Linear Representations of Finite Groups, GTM 42, Springer-Verlag 1977.
[37] J. H. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag 1986.
[38] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, GTM 151, Springer-Verlag 1994.
[39] J. Tate, Number theoretic background, in: Automorphic forms, representations and L-functions, Part 2 (ed. A. Borel and W. Casselman), Proc. Symp. in Pure Math. 33 (AMS, Providence, RI, 1979) 3-26.
[40] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Séminaire Bourbaki, 18e année, 1965/66, no. 306.

Robinson College, Cambridge CB3 9AN, United Kingdom
E-mail address: t.dokchitser@dpmms.cam.ac.uk

Gonville & Caius College, Cambridge CB2 1TA, United Kingdom
E-mail address: v.dokchitser@dpmms.cam.ac.uk